PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-148539
(43)Date of publication of application : 30.05.2000

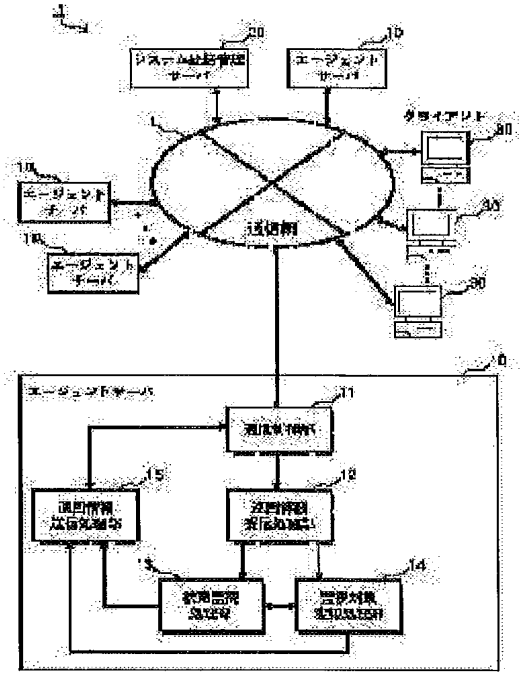
(51)Int.Cl. G06F 11/30
G06F 15/177

(21)Application number : 10-313729
(22)Date of filing : 04.11.1998

(71)Applicant : NTT DATA CORP
(72)Inventor : WATANABE SHINICHI

(54) FAULT DETECTING METHOD, COMPUTER SYSTEM, CONSTITUTIONAL DEVICE, AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a computer system and a constitutional device capable of efficiently detecting the occurrence of a fault in a distributed system.
SOLUTION: In an agent, server 10, a cyclic information receiving processing part 12 decides the sort of a received token and a state monitoring processing part 13 or a monitored object chang-ing processing part 14 generates a corresponding transmission token based on the judged result and agent management information. The generated transmission token is transmitted to another agent server 10 to be a succeeding transmission target in cooperation with a cyclic information transmission processing part 15. The processing part 15 detects the occurrence of a fault in the agent server 10 to be a transmission destination, updates the agent management information and informs a system control management server 20 of the fault accurrence through a communication control part 11.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]While it is the method of detecting existence of a fault occurrence in two or more computer paraphernalia distributed by environment in which two-way communication is possible and each computer paraphernalia receive patrol information sent out from other computer paraphernalia other than self, A process in which patrol information over other computer paraphernalia which are the next sending-out targets based on the patrol information concerned and round hysteresis information held beforehand is generated, While sending out generated patrol information to other computer paraphernalia which are said next sending-out targets, A process in which supervise existence of an obstacle in computer paraphernalia of a transmission destination based on this sent result, and a fault occurrence is detected is performed in this order at least, An obstacle detection method which makes it spread in round to all the computer paraphernalia which had said patrol information distributed, and is characterized by carrying out the health check of the existence of a fault occurrence in specific computer paraphernalia between computer paraphernalia.
[Claim 2]Said patrol information is information formed by either patrol information for surveillance, or patrol information for surveillance object change, and said patrol information for surveillance, A relay interval for controlling transmission time of identification information about computer paraphernalia of a sending out agency, and this patrol information, And are the information formed including a serial number for maintaining the compatibility of this patrol information, and said patrol information for surveillance object change, The obstacle detection method according to claim 1 being the information formed including identification information about computer paraphernalia of a surveillance object added or deleted to environment in which said two-way communication is possible.
[Claim 3]The obstacle detection method according to claim 1 or 2, wherein said patrol information for surveillance object change is information for making changed information over environment by an addition or deletion of specific computer paraphernalia in which said two-way communication is possible spread to all the distributed computer paraphernalia.
[Claim 4]Identification information concerning [said round hysteresis information] self computer paraphernalia, information showing an attainment state to this time of said patrol information in self computer paraphernalia, Information showing operating status about other computer paraphernalia at present, And an obstacle detection method of either of claims 1 thru/or 3 which being the information formed including information showing an influencing state of said patrol information for surveillance object change, and holding for said every computer paraphernalia so that updating is possible given in a paragraph.
[Claim 5]. Based on a gestalt of said distribution for specifying a transfer order of said patrol information, grouping of said round hysteresis information was carried out beforehand. An obstacle detection method of either of claims 1 thru/or 4 being what is formed including information about all the computer paraphernalia used as a surveillance object in a group who belongs self computer paraphernalia given in a paragraph.
[Claim 6]A computer system with an obstacle detection function characterized by what is notified to said 1st computer paraphernalia whenever it has the following and said trouble detecting means detects a fault occurrence.
Connect respectively and the 1st computer paraphernalia that manage in generalization environment in which two-way communication is possible, and two or more 2nd computer

paraphernalia each 2nd computer paraphernalia, A patrol information creating means which generates transmitting patrol information over other 2nd computer paraphernalia that serve as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand while receiving patrol information transmitted from other 2nd computer paraphernalia other than self.
A trouble detecting means which supervises existence of an obstacle in the 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence while transmitting generated transmitting patrol information to other 2nd computer paraphernalia used as said next transmission object.
A fault notification means to notify information about a detected fault occurrence to said 1st computer paraphernalia.

[Claim 7]The computer system according to claim 6, wherein said patrol information creating means is constituted so that said transmitting patrol information of either for surveillance or a for [surveillance object change] may be generated based on classification of said patrol information which received.
[Claim 8]When said patrol information from other 2nd computer paraphernalia other than said self exceeds waiting time set up beforehand based on said round hysteresis information, said patrol information creating means, The computer system according to claim 6 or 7 constituting so that the same transmitting patrol information for surveillance as transmitting patrol information transmitted last time from the 2nd self computer paraphernalia may be generated.
[Claim 9]When said received patrol information is the patrol information for surveillance object change, said patrol information creating means, The computer system according to claim 6 or 7 constituting so that information about other 2nd computer paraphernalia that are based on the patrol information concerned, and are added or deleted to environment in which said two-way communication is possible may be made to reflect in said round hysteresis information and may be updated.
[Claim 10]While said trouble detecting means specifies other 2nd computer paraphernalia that serve as said next transmission object based on said round hysteresis information and transmits said transmitting patrol information, Based on predetermined confirmation-of-receipt information and said round hysteresis information of the 2nd computer paraphernalia of this transmission destination, The computer system according to claim 6 constituting so that existence of a fault occurrence may be detected by judging either ["normal"] or "abnormalities" for operating status in the 2nd computer paraphernalia of this transmission destination.
[Claim 11]When operating status in the 2nd computer paraphernalia of said transmission destination is judged to be "abnormalities", said trouble detecting means, The computer system according to claim 10 which specifies other 2nd computer paraphernalia that serve as a next transmission object further based on said round hysteresis information, and is characterized by being constituted so that the transmitting patrol information concerned may be continued and it may transmit.
[Claim 12]It judges operating status [in / in said fault notification means / the 2nd computer paraphernalia of said transmission destination] "is normal", And when operating status of the 2nd computer paraphernalia of the transmission destination concerned in said round hysteresis information is "abnormalities." The computer system according to claim 10 constituting so that information which expresses restoration of the 2nd computer paraphernalia of the transmission destination concerned to said 1st computer paraphernalia, and which is related with "being normal" may be notified.
[Claim 13]The computer system according to claim 12, wherein said trouble detecting means is constituted so that this transmission result and an obstacle detection result may be made to reflect and said round hysteresis information may be updated ignited by the completion of transmitting of said transmitting patrol information to the 2nd computer paraphernalia of said transmission destination.
[Claim 14]Said 2nd computer paraphernalia patrol information by a token based on predetermined token passing, A computer system of either of claims 6 thru/or 13 which constituting based on said round hysteresis information so that it may be made to go round to said all 2nd computer paraphernalia of corresponding others distributed in environment in which

said two-way communication is possible given in a paragraph.
[Claim 15]A computer system with an obstacle detection function characterized by what is notified to said 3rd computer paraphernalia whenever it has the following and said trouble detecting means detects a fault occurrence.
Two or more 1st computer paraphernalia that become information acquisition request origin in environment in which two-way communication is possible, Two or more 2nd computer paraphernalia that perform an offer of information to said 1st computer paraphernalia, And connect respectively and the 3rd computer paraphernalia that manage in generalization environment in which said two-way communication is possible said 1st and 2nd computer paraphernalia, A patrol information creating means which generates transmitting patrol information over other 1st or 2nd computer paraphernalia that serve as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand while receiving patrol information transmitted from other 1st or 2nd computer paraphernalia other than self.
A trouble detecting means which supervises existence of an obstacle in the 1st or 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence while transmitting generated transmitting patrol information to other 1st or 2nd computer paraphernalia used as said next transmission object.
A fault notification means to notify information about a detected fault occurrence to said 3rd computer paraphernalia.

[Claim 16]The computer system according to claim 6 or 15, wherein environment in which said two-way communication is possible is the wide area network environment which was built by including two or more local network environments in the inside and containing predetermined ISDN which can be contracted out.
[Claim 17]The computer system according to claim 16 constituting based on a communications protocol based on fixed TCP/IP.
[Claim 18]It is respectively connected to the 1st computer paraphernalia that manage in generalization environment in which two-way communication is possible, and two or more 2nd computer paraphernalia, It is the recording medium which recorded a program code as which it is read by said 2nd specific computer paraphernalia, and the computer paraphernalia concerned are operated as an operating condition monitoring device to said other 2nd computer paraphernalia, While receiving at least patrol information transmitted from other 2nd computer paraphernalia other than self, said program code, Processing which generates transmitting patrol information over other 2nd computer paraphernalia used as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand, While transmitting generated transmitting patrol information to other 2nd computer paraphernalia used as said next transmission object, Processing which supervises existence of an obstacle in the 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence, A recording medium being a thing which makes said 2nd computer paraphernalia perform processing which notifies information about a detected fault occurrence to said 1st computer paraphernalia.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a system management and obstacle detection art, and relates to the technique of reducing in more detail the traffic which starts data communications in the network environment of a distributing system, and detecting the fault occurrence in computer paraphernalia efficiently.
[0002]
[Description of the Prior Art]In recent years, development of the computer system which performs an offer of information with various gestalten to a user by development of the large-scale and high-speed network environment represented by communications networks, such as the Internet, is prosperous. In these computer systems, the system construction of high reliability and system management management in consideration of the degradation of the whole system accompanying a fault occurrence, the security to the unauthorized entry person to a system, etc. are desired.
[0003]Two or more computer paraphernalia which take charge of execution of characteristic processing, maintenance of information, etc., for example are distributed and arranged on a network, and the distributing system which aims at improvement in the processing efficiency in the whole system is known for such a computer system. In this distributing system, the client/server system type communication configuration is adopted, and a user uses the interface for access from the computer paraphernalia used as a client side, accesses a server, and usually acquires desired electronized information.
[0004]As one gestalt of the construction in a distributing system, a network environment is built with the large-scale WAN (Wide Area Network) environment having contained two or more LAN (Local Area Network), for example, While making each server which takes charge of characteristic processing of a WWW (World Wide Web) server, DNS (Domain Name System), a Proxy server, etc. distribute on this WAN, The system management technique which performs unitary operation management with the generalization managing server which manages the whole system in generalization is known.
[0005]In such a system management technique, by checking each agent's starting mentioned later, a generalization managing server supervises an agent's operating status, and detects a fault occurrence. In order to perform central control from the surveillance manager generalization managing server which specifically supervises the generalization operating status over two or more computer paraphernalia, such as a server used as a surveillance object, In each server machine which were distributed, the surveillance application called a surveillance agent (it is only hereafter described as an "agent") is stationed permanently. The "event-driven method" is usually adopted as the agent.
Only when a fault occurrence is detected in an agent, that is notified to a generalization managing server.

[0006]Although there is a merit which makes the traffic between an agent and a generalization managing server and the resource usage rate of a generalization managing server reduce in this event-driven method, when there is no notice from a specific agent in a generalization managing server, while the agent concerned is working normally, there is no notice -- or whether the agent concerned has stopped and there is any notice cannot judge from a generalization managing

server.
[0007]Some obstacle detection techniques are proposed though it is an event-driven method in order to solve such a problem, and so that it may be possible to get to know two or more agents' operating status in real time in a generalization managing server. Hereafter, with reference to drawings, the outline is explained about the conventional obstacle detection technique. The data communications between a generalization managing server and an agent shall be based on the remote access via a network.
[0008](1) Polling drawing 9 from a generalization managing server is a figure showing one embodiment in the distributing system of a conventional type. In order that a generalization managing server may check each agent's starting, while performing an inquiry of a seizing acknowledgment, i.e., polling, periodically to the agent of each machine which serves as a surveillance object from the generalization managing server side, each agent returns a check to this inquiry. Since the check to a generalization managing server does not return when abnormalities etc. occur to an agent, in the generalization managing server side, the obstacle detection in the agent concerned is attained ignited by this check impossible.
[0009](2) Process health check drawing 10 within a surveillance object machine is a figure showing the health check between the processes in the computer paraphernalia of a conventional type. The health check between the agent processes in the specific computer paraphernalia (a "machine" is called hereafter) which constitute a distributing system is expressed with this figure. This technique detects obstacles, such as a down of an agent process, by supervising mutually whether two or more agent processes were respectively started inside each machine used as a surveillance object, and each agent process has started mutually. For example, since it is constituted so that a reboot of the agent process in which other agent processes were downed is possible when a specific agent process is downed, prevention in the state where an agent process continues being downed is attained. Simultaneously with down detection of a specific agent process, since this fault occurrence is notified to a generalization managing server from other agent processes, the obstacle detection to the machine from the generalization managing server side is attained.
[0010](3) Sub generalization managing server installation drawing 11 is a figure showing one gestalt of the operation in the distributing system of a conventional type. In the usual distributing system, since two or more surveillance object machines are installed in the same LAN in many cases, two or more agent itself exists. Then, this technique is constituted so that the specific agent in two or more surveillance object machines may achieve the function as a sub generalization managing server in LAN. The agent who functions as a sub generalization managing server notifies the fault occurrence of the agent concerned to a generalization managing server, when it asks for every fixed time to other agents and the check from a specific agent does not return. In a generalization managing server, the obstacle of the surveillance object machine concerning an agent [/ ignited by this notice] is detected.
[0011]
[Problem(s) to be Solved by the Invention]By the way, there was a problem as shown below in the obstacle detection technique in an above-mentioned distributing system.
(1) Since the traffic applied to polling with the increase in the number of polling agents from a generalization managing server also increases, the load in a network increases. In this case, although some solutions can be performed by lengthening the interval of polling, the real time nature in a distributing system will be spoiled. When a generalization managing server and the network between agents are WAN like ISDN (Integrated Services Digital Network), since it will be charged for every polling, there is the necessity for a system construction of having taken economical efficiency into consideration.
[0012](2) Although an agent's prevention from a down is attained in the same machine used as the process mutual surveillance surveillance object within a surveillance object machine, management about the case where the machine itself [concerned] is downed cannot be performed.
[0013](3) When the agent who functions as a sub generalization managing server installation sub generalization managing server is downed, it becomes impossible grasping other agents' operating status which the agent concerned made the surveillance object. When this is coped with and two or more agents of a sub generalization managing server are installed, network load increases and

judgment of the trade-off becomes difficult. Since the information which agent a sub generalization managing server supervises is also needed, the amount of signal transduction which is needed with the increase in the number of sub generalization managing servers also increases.

[0014]Such a problem will be solved if the distributing system in consideration of the communications traffic between a generalization managing server and an agent and the utilization ratio of the resource can be built about detection of a fault occurrence.

[0015]Then, there is a technical problem of this invention in providing the obstacle detection method which becomes detectable [the efficient fault occurrence in a distributing system]. There are other technical problems of this invention in providing a computer system suitable for operation of the above-mentioned obstacle detection method, and its component. There are other technical problems of this invention in providing a recording medium for general-purpose computer paraphernalia to realize the above-mentioned obstacle detection method, a computer system, etc.

[0016]

[Means for Solving the Problem]An obstacle detection method of this invention which solves an aforementioned problem, While it is the method of detecting existence of a fault occurrence in two or more computer paraphernalia distributed by environment in which two-way communication is possible and each computer paraphernalia receive patrol information sent out from other computer paraphernalia other than self, A process in which patrol information over other computer paraphernalia which are the next sending-out targets based on the patrol information concerned and round hysteresis information held beforehand is generated, While sending out generated patrol information to other computer paraphernalia which are said next sending-out targets, A process in which supervise existence of an obstacle in computer paraphernalia of a transmission destination based on this sent result, and a fault occurrence is detected is performed in this order at least, It is made to spread in round to all the computer paraphernalia which had said patrol information distributed, and the health check of the existence of a fault occurrence in specific computer paraphernalia is carried out between computer paraphernalia.

[0017]The contents of each above-mentioned information are as follows.

(1) Patrol information : information formed by either patrol information for surveillance, or patrol information for surveillance object change.

(2) Patrol information for surveillance : information formed including a serial number for maintaining a relay interval for controlling transmission time of identification information about computer paraphernalia of a sending out agency, and the above-mentioned patrol information, and the compatibility of the patrol information.

(3) Patrol information for surveillance object change : information formed including identification information about computer paraphernalia of a surveillance object added or deleted to environment in which said two-way communication is possible. This patrol information for surveillance object change is information for making changed information over environment by an addition or deletion of specific computer paraphernalia in which said two-way communication is possible spread to all the distributed computer paraphernalia.

Round hysteresis information : (4) Identification information about self computer paraphernalia, information showing an attainment state to this time of said patrol information in self computer paraphernalia, It is the information formed including information showing operating status about other computer paraphernalia at present, and information showing an influencing state of said patrol information for surveillance object change, and for said every computer paraphernalia, is held so that updating is possible. This round hysteresis information may be formed including information about all the computer paraphernalia used as a surveillance object in a group who belongs self computer paraphernalia by which grouping was beforehand carried out based on a gestalt of said distribution for specifying a transfer order of said patrol information.

[0018]A computer system of this invention which solves a technical problem besides the above, The 1st computer paraphernalia that manage in generalization environment in which two-way communication is possible, and two or more 2nd computer paraphernalia are connected respectively. While receiving patrol information transmitted from other 2nd computer paraphernalia other than self, each 2nd computer paraphernalia, A patrol information creating

means which generates transmitting patrol information over other 2nd computer paraphernalia used as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand, While transmitting generated transmitting patrol information to other 2nd computer paraphernalia used as said next transmission object, A trouble detecting means which supervises existence of an obstacle in the 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence, Whenever it has a fault notification means to notify information about a detected fault occurrence to said 1st computer paraphernalia and said trouble detecting means detects a fault occurrence, it is a computer system with an obstacle detection function characterized by what is notified to said 1st computer paraphernalia.

[0019]Said patrol information creating means is constituted so that said transmitting patrol information of either for surveillance or a for [surveillance object change] may be generated for example, based on classification of said patrol information which received. Or when said patrol information from other 2nd computer paraphernalia other than said self exceeds waiting time set up beforehand based on said round hysteresis information, it is constituted so that the same transmitting patrol information for surveillance as transmitting patrol information transmitted last time from the 2nd self computer paraphernalia may be generated. Or when said received patrol information is the patrol information for surveillance object change, it is constituted so that information about other 2nd computer paraphernalia that are based on the patrol information concerned, and are added or deleted to environment in which said two-way communication is possible may be made to reflect in said round hysteresis information and may be updated.

[0020]While said trouble detecting means specifies other 2nd computer paraphernalia that serve as said next transmission object based on said round hysteresis information and transmits said transmitting patrol information, Based on predetermined confirmation-of-receipt information and said round hysteresis information of the 2nd computer paraphernalia of this transmission destination, by judging either ["normal"] or "abnormalities" for operating status in the 2nd computer paraphernalia of this transmission destination, it is constituted so that existence of a fault occurrence may be detected. In this trouble detecting means, when operating status is judged to be "abnormalities", based on said round hysteresis information, other 2nd computer paraphernalia that serve as a next transmission object further are specified, and the transmitting patrol information concerned is continued and it transmits. Information which it judges operating status "is normal", and expresses restoration of the 2nd computer paraphernalia of the transmission destination concerned to said 1st computer paraphernalia when operating status of the 2nd computer paraphernalia of the transmission destination concerned in said round hysteresis information is "abnormalities" and which is related with "being normal" is notified. Ignited by the completion of transmitting of said transmitting patrol information to the 2nd computer paraphernalia of said transmission destination, this transmission result and an obstacle detection result are made to reflect, and said round hysteresis information is updated.

[0021]Said 2nd computer paraphernalia patrol information by a token based on predetermined token passing, for example, Based on said round hysteresis information, it is constituted so that it may be made to go round to said all 2nd computer paraphernalia of corresponding others distributed in environment in which said two-way communication is possible.

[0022]Two or more 1st computer paraphernalia that become information acquisition request origin in environment in which two-way communication of other computer systems of this invention is possible, Two or more 2nd computer paraphernalia that perform an offer of information to said 1st computer paraphernalia, And the 3rd computer paraphernalia that manage in generalization environment in which said two-way communication is possible are connected respectively. While receiving patrol information transmitted from other 1st or 2nd computer paraphernalia other than self, said 1st and 2nd computer paraphernalia, A patrol information creating means which generates transmitting patrol information over other 1st or 2nd computer paraphernalia used as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand, While transmitting generated transmitting patrol information to other 1st or 2nd computer paraphernalia used as said next transmission object, A trouble detecting means which supervises existence of an obstacle in the 1st or 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence, . It is characterized by what is notified to said 3rd computer paraphernalia whenever

it has a fault notification means to notify information about a detected fault occurrence to said 3rd computer paraphernalia and said trouble detecting means detects a fault occurrence. It is a computer system with an obstacle detection function.
[0023]A recording medium of this invention which solves a technical problem besides the above, It is respectively connected to the 1st computer paraphernalia that manage in generalization environment in which two-way communication is possible, and two or more 2nd computer paraphernalia, It is the recording medium which recorded a program code as which it is read by said 2nd specific computer paraphernalia, and the computer paraphernalia concerned are operated as an operating condition monitoring device to said other 2nd computer paraphernalia, While receiving at least patrol information transmitted from other 2nd computer paraphernalia other than self, said program code, Processing which generates transmitting patrol information over other 2nd computer paraphernalia used as a next transmission object based on the patrol information concerned and round hysteresis information held beforehand, While transmitting generated transmitting patrol information to other 2nd computer paraphernalia used as said next transmission object, Said 2nd computer paraphernalia are made to perform processing which notifies information about a fault occurrence which supervises existence of an obstacle in the 2nd computer paraphernalia of a transmission destination based on this transmission result, and detects a fault occurrence, and which was processed and detected to said 1st computer paraphernalia.
[0024]
[Embodiment of the Invention]Hereafter, with reference to drawings, an embodiment of the invention is described in detail.
(A 1st embodiment) Drawing 1 is a functional block diagram showing the embodiment at the time of applying this invention to the computer system which performs an offer of information. This computer system 1 distributes and arranges two or more agent servers 10, the system generalization managing server 20 which performs generalization management of the whole system, and two or more clients 30, and via the communications network L, respectively, it is connected so that two-way communication is possible, and it is constituted. The communications network L in this case is the wide area network environment by WAN containing ISDN etc. which can be contracted out built by including local network environments, such as two or more LAN, in that inside, for example.
[0025]While the agent server 10 is an operating server which provides the service about the peculiar application and information which the computer paraphernalia which constitute the server concerned held to two or more clients 30, It functions as what is called an operating condition monitoring device that supervises operating status in between [two or more] agent server 10. Each server function in two or more agent servers 10 is constituted, for example so that DNS, Proxy, WINS (Windows Internet Network Service), a database management system (DBMS), etc. may be provided.
[0026]Hereafter, by this embodiment, the explanation about the server function to the client 30 realized by known art is omitted about the functional constitution in the agent server 10, and the functional constitution as an operating condition monitoring device between two or more agent servers 10 is explained. The data access between two or more agent servers 10 shall be due to the publicly known token passing technique (Token Passing Method) which makes a network patrol in order of the node beforehand set up in the message by a predetermined token.
[0027]The system generalization managing server 20 is a server which manages the computer system 1 whole in generalization, and is positioned as a surveillance manager to two or more agent servers 10. When an obstacle occurs in the specific agent server 10, specifically, The system generalization managing server 20 which was based on the notice of the fault occurrence made from other agent servers 10, and detected the obstacle is constituted so that an administrator may be notified in the information about this obstacle or it may leave record (log).
[0028]In the information retaining means which is not illustrated, the system generalization managing server 20 holds the surveillance management information about two or more agent servers 10. An example of the construction form in surveillance management information is shown in drawing 2. "Agent ID" is the identification information given respectively every agent server 10 among a figure, and surveillance management information is built from the group with the "IP address" of "agent ID" and the corresponding agent server 10. In this case, as for

"agent ID", in order to decide on a meaning and to use in order of transfer of a token within the surveillance group set up beforehand, it is desirable that it is a numerical value. So that the agent servers which a surveillance group is a set of the agent server for performing the health check of operating status among two or more agent servers 10, and were left in network may not supervise each other, What is necessary is just to build as an agent server group belonging to the same site preferably based on the distributed form like the same LAN, a segment, etc. From this, the surveillance management information about all the surveillance groups is held with the system generalization managing server 20.

[0029]The computer system 1 in this embodiment shall be constituted based on the communications protocol of publicly known TCP/IP (Transmission Control Protocol/Internet Protocol). However, it may not be limited to such an example but may be constituted based on the communications protocol of UDP.

[0030]The agent server 10 which is realized by computer paraphernalia and which functions as an operating condition monitoring device, The communication control part 11, the patrol information receiving processing part 12, the condition-monitoring treating part 13 and the surveillance object change processing part 14 which are formed by reading and executing a predetermined program under self OS, and the patrol information transmission processing part 15 are provided, and it is constituted.

[0031]The above-mentioned program in which each function in the agent server 10 is made to form, Usually, it is stored in the inside or external storage of computer paraphernalia which constitutes the agent server 10 concerned by the arbitrary recording forms which can form each above-mentioned functional block, and it is read at any time and performs. For example, portable recording media, such as CD-ROM with disengageable computer paraphernalia etc., and FD, Or it may be stored in the program server etc. which were connected to the local area network with a computer-readable gestalt, it may be installed in the inside or external storage of the above-mentioned computer paraphernalia at the time of use, and execution may be presented at any time. The above-mentioned functional blocks 11-15 may be suitably realized by the formation by the above-mentioned program independent, or accessory movement with the operating system carried in computer paraphernalia.

[0032]The communication control part 11 performs data transfer with the system generalization managing server 20 and two or more agent servers 10 via the communications network L.

[0033]The response indication which patrols the patrol information receiving processing part 12 from two or more agent servers 10 used as the surveillance object of operating status, and is made, namely, -- while receiving via the communication control part 11 based on the agent management information which mentions a token (henceforth, receiving token) later -- the classification of the receiving token concerned -- "the token for surveillance" -- or "the token for change" is judged.

[0034]When the receiving token in the patrol information receiving processing part 12 is "a token for surveillance", the condition-monitoring treating part 13, While generating based on the agent management information which mentions later the transmission token for agent server surveillance which next time should be made to patrol, The token concerned is transmitted to other agent servers 10 which serve as a transmission object via the communication control part 11 by moving together with the patrol information transmission processing part 15.

[0035]The receiving token in the patrol information receiving processing part 12 the surveillance object change processing part 14, In the case of "the token for change" showing the addition or deletion about the specific agent server 10 used as a surveillance object, While generating based on the agent management information which mentions later the transmission token for agent server change which next time should be made to patrol, The token concerned is transmitted to other agent servers 10 which serve as a transmission object via the communication control part 11 by moving together with the patrol information transmission processing part 15.

[0036]While the patrol information transmission processing part 15 transmits the transmission token respectively generated in the condition-monitoring treating part 13 and the surveillance object change processing part 14 to other agent servers 10 which serve as a transmission object via the communication control part 11, Based on this transmission result and the agent management information mentioned later, the operating status in the transmission destination agent server 10 of the token concerned is judged. It is constituted so that this decision result

may be notified to the system generalization managing server 20 via the communication control part 11. Whenever it specifically detects the case where transmission is impossible, as a fault occurrence in the agent server 10 concerned to the transmission destination agent server 10 which should make a transmission token patrol, the information about this obstacle detection is notified to the system generalization managing server 20.

[0037]In this case, a transmission token is continued and transmitted to the next of the agent server 10 with which the obstacle was detected to other agent servers 10 used as a transmission object, It is constituted so that it may transmit again, when the transmission token has gone round to the self agent server 10 to the same agent server 10 with which the obstacle was detected.

[0038]Next, the agent management information in the agent server 10 is explained. The agent server 10 operates the above-mentioned functional blocks 11-15 based on the agent management information concerned while holding the agent management information beforehand built in the information control means which is not illustrated.

[0039]An example of the construction form in agent management information is shown in drawing 3. "Agent ID" and an "IP address" correspond to the surveillance management information in the above-mentioned system generalization managing server 20 among a figure, and a transfer order of a token is determined based on this "agent ID." What is necessary is just to build the "IP address" corresponding to "agent ID" used as a missing number in agent management information, so that a zero clear may be carried out.

[0040]"Operating status" is the information showing whether it is working or not, and the agent server 10 corresponding in this time this "operating status", There should be only information about the agent server 10 which did not need to hold the information about the operating status of all the agent servers 10, for example, transmitted the token to the past from the self agent server 10.

[0041]It is the information showing whether the "transfer flag" was transmitted to the agent server 10 with which information, including the IP address of the agent server 10 concerned, etc., should make next time patrol a token, when a change of an addition, deletion, etc. about the specific agent server 10 was made. The information about the changed agent server 10 is transmitted in round by the transmission token from other agent servers 10 with which transmission was made to the self agent server 10. Since each agent server 10 needs to have the "surveillance group list" information about all the agent servers 10 which constitute a surveillance group, maintenance of the latest information is realized by this "transfer flag." On the other hand, "the waiting time for a token" and a "token serial number" are information in order to detect the mismatching about a token, and the error on communication.

[0042]This agent management information is used as hysteresis information of the round about the token of the agent server 10 at present. What is necessary is just to build the data structure in agent management information suitably with corresponding gestalten, such as a tabular format and list form, without limiting to the above-mentioned example of construction.

[0043]Thus, each agent server 10 should just hold the agent management information about the surveillance group to whom self belongs, The health check of operating status and automatic transfer of the configuration change information in the specific agent server 10 are realized by the agent management information concerned and the token which patrols between the agent servers 10.

[0044]Next, the token which patrols between the agent servers 10 is explained. Drawing 4 is a mimetic diagram showing the outline of the monitoring process of the operating status between the agent servers 10. At this embodiment, the token which patrols the computer system 1, i.e., a transmission token, patrols between the agent servers 10 with two kinds of gestalten so that it may illustrate. In the patrol information receiving processing part 12 in the agent server 10. A transmission token is received and "the tokens for change", such as an addition, deletion, etc. about "the token for surveillance" usual in the token concerned or the specific agent server 10, is judged from the flag showing the "processing classification" included in the token concerned.

[0045]"The token for surveillance" is constituted including the "serial number" for maintaining the "relay interval" showing the round delay for controlling the flag "processing classification", "transmitting agency agent ID", and the transmitting processing time of a token showing the token for surveillance, and the compatibility of a token. Whenever it takes a round of a

surveillance group, when it is constituted so that that value may increase and a serial number increases a "relay interval", the "serial number" in this case so that a token may not flow too much, In the agent server 10, the value computed by having considered time to take a round from "the waiting time for a token" of agent management information and actual time is given.
[0046]On the other hand, "the token for change" is constituted including the flag "processing classification" showing the token for change, "change agent ID" added or deleted to the communications network L in the computer system 1, and corresponding "change IP address." In this case, it is constituted so that it may judge with "deletion" of the corresponding agent server 10, and a "addition" of the agent server 10 which corresponds in the case of the other value, when a "change IP address" is "0" for example.
[0047]Since transmission of the transmission token to the agent server C of agent ID "003" was [in / with this figure / the surveillance group A] impossible, It means that the obstacle in the agent server C concerned is detected by the agent server B of agent ID "002" which becomes a transmitting agency, and the notice to the system generalization managing server 20 is made.
[0048]Next, concrete operation of the computer system 1 in this embodiment is explained. Drawing 5 – 8 are the procedure figures in the computer system 1. First, the outline procedure in the agent server 10 shown in drawing 5 is explained. The patrol information receiving processing part 12 of the agent server 10 detects the waiting time which starts reception of a token based on agent management information (Step S101). When received, without the waiting time concerned exceeding "the waiting time for a token" in agent management information (Step S101: receive, without exceeding), the patrol information receiving processing part 12 receives the token concerned, and judges the classification (step S102-103).
[0049]When the classification of the judged receiving token is "a token for surveillance", (the token for step S103:surveillance) and the patrol information receiving processing part 12, Processing is suspended based on the "relay interval" in the token concerned, or the "token waiting time" in agent management information (Step S104). The traffic in the communications network L is controlled by [this / that carries out time standby] having been specified "at intervals of the relay." Next, a control is moved from the patrol information receiving processing part 12 to the condition-monitoring treating part 13, and the monitoring process between the agent servers 10 is performed (Step S105). The monitoring process concerned is mentioned later.
[0050]After completing the monitoring process concerned, the agent server 10 repeats return processing to Step S101 while it re-computes "token waiting time" by the information control means which is not illustrated based on this monitoring process result and updates agent management information (Step S106). When the receiving token in the patrol information receiving processing part 12 is "a token for change", change processing about the agent server 10 which (the token for step S103:change) and a control are moved to the surveillance object change processing part 14, and is mentioned later is performed (Step S107).
[0051]On the other hand, when a token exceeds waiting time and is received in the above-mentioned step S101, (step S101: It exceeded), Since a certain abnormalities -- the existence of the agent server 10 and the communications network L which obstacles, such as a down, generated with the token held were divided -- can be predicted, in the condition-monitoring treating part 13, the same transmission token for surveillance as last time is generated (Step S108). It is transmitted to other agent servers 10 which the token concerned moves together with the patrol information transmission processing part 15, and serve as a transmission object from the self agent server 10 next time, While re-computing "token waiting time" by the information control means which is not illustrated and updating agent management information (step S109-110), return processing is repeated to Step S101.
[0052]In this case, other agent servers 10 used as a next transmission object are the agent servers 10 with which "agent ID" in the surveillance group list of agent management information serves as a large value after agent ID of self. When agent ID used as a larger value than self-agent ID does not exist in agent management information, the patrol information transmission processing part 15, For example, it is constituted so that the next transmission object agent server 10 may be specified based on agent ID used as the minimum in a surveillance group. By this processing, the source of release of an obstacle is specified from the token again patrolled to the self agent server 10. Transmitting processing of a token is mentioned later.

[0053]Next, the condition-monitoring procedure in the agent server 10 shown in drawing 6 is explained. It is judged whether the condition-monitoring treating part 13 is larger than the "token serial number" in the agent management information by which the "serial number" was held to the receiving token from the patrol information receiving processing part 12 at the self-agent server 10 (Step S201). When judged with carrying out "1" increment from what compared the "serial number" of the receiving token with the "token serial number" in agent management information, and specifically received last time, (Step S201:Yes), The "transfer flag" with which agent management information corresponds based on "transmitting agency agent ID" in the token concerned is checked (Step S203). On the other hand, since it means that (Step S201:No) and the receiving token concerned are going round doubly when the "serial number" of the receiving token has not carried out increment from the "token serial number" in agent management information, the receiving token concerned is canceled (Step S202).
[0054]By next, the check of a "transfer flag". [in / at the condition-monitoring treating part 13 / agent management information] When judged with there being change to the corresponding agent server 10, it moves together with (Step S203: It is subject to change to an agent), and the surveillance object change processing part 14, and the token for change is generated (Step S204). It is constituted so that the "change IP address" in the token for change may specifically be set up by the IP address of the agent server 10 with the change corresponding to a "transfer flag."
[0055]The "transfer flag" which the generated token for change is transmitted to other agent servers 10 which serve as a next transmission object by the patrol information transmission processing part 15, and corresponds in agent management information is cleared ignited by this completion of transmitting by the information control means which is not illustrated. (Step S205-206).
[0056]Next, in the condition-monitoring treating part 13, agent ID of self is set as "transmitting agency agent ID", and the token for surveillance is generated (Step S207). The condition-monitoring treating part 13 compares "transmitting agency agent ID" in a receiving token with agent ID of self. When "transmitting agency agent ID" is below agent ID of self, (Step S208:No), While setting up the "token serial number" in agent management information to the "serial number" of the token for surveillance (Step S209), the "relay interval" of the token for surveillance is set up (Step S210).
[0057]On the other hand, when "transmitting agency agent ID" is more than agent ID of self, (Step S208:Yes) and the condition-monitoring treating part 13, While carrying out "1" increment of the "token serial number" in agent management information and setting up the "serial number" of the token for surveillance (Step S211), Based on the "token waiting time" in agent management information, and actual time, the "relay interval" of the token for surveillance is set up (Step S212).
[0058]According to the "serial number" set up to the token for surveillance in the information control means which is not illustrated in the above-mentioned step S208 - 212. While updating and holding the "token serial number" in agent management information (Step S213), in the patrol information transmission processing part 15, the set-up token for surveillance is transmitted to the agent server 10 which serves as a transmission object via the communication control part 11 (Step S214).
[0059]Next, the change processing procedure about the specific agent server 10 shown in drawing 7 is explained. When the change to the computer system 1 by an addition or deletion of the specific agent server 10 is made, This change is made to reflect to the agent management information which each agent server 10 corresponding to the surveillance group to whom the agent server concerned should belong holds, and it must update. In this case, changed information, such as an addition and deletion, is not transmitted to each agent server 10 from the system generalization managing server 20, but agent server 10 self used as a change target transmits the changed information concerned to other agent servers 10 used as a next transmission object by a token. by this processing, to all the agent servers 10 in the computer system 1, the changed information concerned is boiled and that including the agent server 10 with which obstacles, such as a down, are detected spreads.
[0060]In agent server 10 addition, The newest surveillance group list and agent ID of self shall be beforehand given from the system generalization managing server 20 at the time of this addition,

and in agent server 10 deletion, The token for change shall be generated based on agent ID of self in agent management information.

[0061]First, the surveillance object change processing part 14 sets up the IP address of the receiving token concerned in the surveillance group list of agent management information to the "IP address" corresponding to "agent ID" of a receiving token (Step S301). The surveillance object change processing part 14 sets up the "transfer flag" corresponding to "agent ID" of a receiving token in agent management information (Step S302). Next, while the surveillance object change processing part 14 generates "the token for change" which set up the IP address of the agent server 10 with change as a "change IP address" (Step S303), It moves together with the patrol information transmission processing part 15, and the token concerned is transmitted to the agent server 10 used as a next transmission object (Step S304).

[0062]In the patrol information transmission processing part 15, the "transfer flag" with which it moves together with the information control means which is not illustrated ignited by the completion of transmitting of "the token for change", and agent management information corresponds is cleared (Step S305). In this case, what is necessary is just to constitute so that the clearance to a "transfer flag" may not be performed although the token for change is transmitted to the agent server 10 which serves as a next transmission object further when other agent servers 10 used as a next transmission object are downed for example.

[0063]From the above processing, agent server 10 self used as change targets, such as an addition and deletion, Without transmitting to all the agent servers 10, what is necessary is to transmit only to the agent server 10 used as at least one transmission object, and the token for change with the token and the "transfer flag" to patrol. Corresponding changed information spreads certainly to all the agent servers 10.

[0064]Next, the transmitting procedure of the token shown in drawing 8 is explained. The patrol information transmission processing part 15 acquires a next transmission object, i.e., the IP address of the agent server 10 which should next make a token patrol, from the surveillance group list of agent management information (Step S401). When a next transmission object is the self agent server 10, (Step S402:Yes) and the abnormal value showing an error are returned. On the other hand, when a next transmission object is except agent server 10 of self (Step S402: No), the patrol information transmission processing part 15 transmits a token to the agent server 10 concerned via the communication control part 11 (Step S403).

[0065]Next, the patrol information transmission processing part 15 judges the transmission result of a token via the communication control part 11. When the token concerned is transmitted normally, (Step S404:Yes), the case where "operating status" of the agent server 10 with which the token concerned was transmitted in agent management information is checked, and the "operating status" concerned is "normal" -- (-- step S405:normal) and normal values are returned.

[0066]On the other hand, it is reported when the "operating status" concerned is "abnormalities" (Step S405: abnormalities), the patrol information transmission processing part 15 "is normal" in the agent server 10 corresponding to the system generalization managing server 20 (Step S406). The patrol information transmission processing part 15 updates the "operating status" about the agent server 10 with which it moves together with the information control means which is not illustrated, and agent management information corresponds "for it to be normal" (Step S407). By this step S405 - processing of 407, the notice of "restoration" about the agent server 10 in which transmission of the token had failed is made to the system generalization managing server 20 to last time. [what is called]

[0067]When a token is not able to transmit normally in the above-mentioned step S404 (Step S404: No), the patrol information transmission processing part 15, The last "operating status" about the agent server 10 of a transmission destination in agent management information is judged, the case where these decision results are "abnormalities" -- (-- it returns to step S408:unusual) and Step S401, the agent server 10 which serves as a next transmission object further is specified, and processing is repeated.

[0068]On the other hand, when "operating status" is "normal" (Step S408: normal), the patrol information transmission processing part 15 notifies the obstacle detection in the agent server 10 concerned to the system generalization managing server 20 (Step S409). The patrol information transmission processing part 15 moves together with the information control means

which is not illustrated, and updates the "operating status" in agent management information to "abnormalities" (Step S410).
[0069]As the check technique about the transmission result of the token in the above-mentioned step S404, It may constitute so that the transmission result of a token may be judged based on the response including the confirmation-of-receipt information made from the agent server 10 side of a transmission destination in the patrol information transmission processing part 15 using TCP which is connection-oriented communication, or UDP of a connectionless type, for example.
[0070]Thus, in the computer system 1 of this embodiment. While making a token patrol among two or more agent servers and carrying out the health check of the operating status in each agent server, Only when the obstacle in a specific agent server is detected, from this obstacle detection being notified from other agent server side to a system generalization managing server. The communications traffic in a network environment can be reduced without performing polling from a system generalization managing server like conventional method.
[0071]Since operating status is mutually supervised based on the token patrolled between agent servers, while grasp becomes certainly possible in real time mostly, the activation status of each agent server, For example, the down of the agent server device itself, the down of the agent process in an agent server, etc. are detectable as a fault occurrence.
[0072]Since all the agent servers in a network environment are in the same position, load sharing becomes possible, without the traffic which starts the surveillance of operating status as compared with conventional method concentrating.
[0073]Since it is notified to a system generalization managing server only when an obstacle is detected in an agent server, the network load between a system generalization managing server and an agent server and the usage rate of a resource are reduced remarkably.
[0074]When contracting out for example, while the always-on connection with a network becomes unnecessary in the distributing system which went via WAN, Since the operating status in an agent server can be notified to a system generalization managing server by necessary minimum communication, communication cost is reduced and economic effectuation improves substantially.
[0075]Changed information, such as an addition, deletion, etc. about the specific agent server used as a surveillance object, Since the agent server concerned itself makes it go round to other agent server groups by a token, it becomes possible to make the changed information concerned affect a network environment, without a system generalization managing server involving.
[0076]Even if it is a case where obstacles, such as a down, have occurred in a specific agent server, based on the token to patrol, the transfer of the automatic information over other agent server groups of a system generalization managing server is attained, without involving. Thus, according to the computer system 1 of this embodiment, the processing efficiency concerning the reliability and operation management in the whole system improves substantially.
[0077](A 2nd embodiment) For example, it is made to apply to two or more clients which can be set to a client/server system, and this invention can also be constituted. The client in this case possesses at least the patrol information receiving processing part 12 which is the same functional block as the agent server 10 in the above-mentioned computer system 1, the condition-monitoring treating part 13, the surveillance object change processing part 14, and the patrol information transmission processing part 15, and is constituted.
[0078]The point that this client is different from the agent server 10, For example, it is the point of providing the display for showing the information about the fault occurrence detected to the client, and a client is made to constitute so that a message etc. may be outputted to output units, such as a display device provided in a client. Substitution of the processing equivalent to the communication control part 11 is attained by using the function of communications control to provide in the client itself.
[0079]The agent server 10 in a 1st embodiment, As mentioned above, the health check of operating status is performed among two or more agent servers, and all the agent servers 10 are positioned as a peer level from a viewpoint of a hierarchy of system in the computer system 1. By a 2nd embodiment, as the agent server 10 and computer paraphernalia of a peer level, make two or more clients function them respectively, and from this, for example like, The above-mentioned functional blocks 12-15 are made to incorporate and provide, and it becomes possible

by constituting a client to acquire an effect equivalent to the agent server 10 in the above-mentioned computer system 1.

[0080]When the above-mentioned computer system 1 is built using the client of this embodiment, All the computer paraphernalia other than the above-mentioned system generalization managing server 20 serve as a peer level, and the health check of the operating status between two or more clients, between two or more agent servers 10, and between a client - the agent server 10 of them becomes possible.

[0081]

[Effect of the Invention]According to this invention, there is a characteristic effect of becoming detectable [the efficient fault occurrence in a distributed type computer system] so that clearly from the above explanation. According to the computer system of this invention, since the health check of operating status can be performed between the computer paraphernalia which constitute a distributing system, system management management environment with high reliability and processing efficiency has an effect which becomes realizable.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The functional block diagram showing one embodiment of the computer system of this invention.
[Drawing 2]An example of the construction form in surveillance management information.
[Drawing 3]An example of the construction form in agent management information.
[Drawing 4]The mimetic diagram showing the outline of the monitoring process of this embodiment.
[Drawing 5]The procedure figure in the agent server of this embodiment.
[Drawing 6]The procedure figure in condition-monitoring processing.
[Drawing 7]The procedure figure in agent change processing.
[Drawing 8]The procedure figure in token transmitting processing.
[Drawing 9]The figure showing one embodiment in the distributing system of a conventional type.

[Drawing 10]The figure showing the health check between the processes in the computer paraphernalia of a conventional type.
[Drawing 11]The figure showing one embodiment in the distributing system of a conventional type.
[Description of Notations]
1 Computer system
10 Agent server
11 Communication control part
12 Patrol information receiving processing part
13 Condition-monitoring treating part
14 Surveillance object change processing part
15 Patrol information transmission processing part
20 System generalization managing server
30 Client
L Communications network

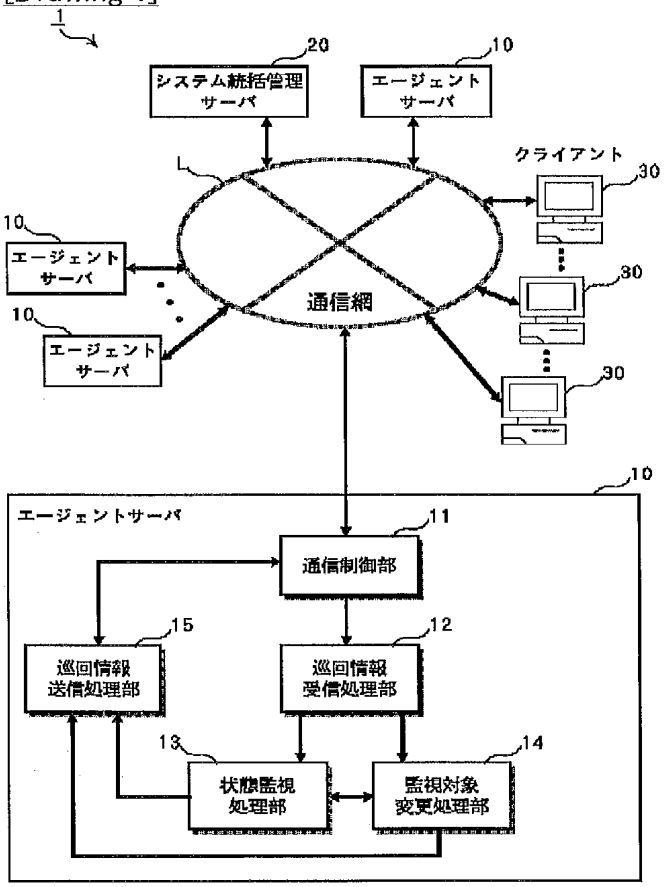
[Translation done.]

* NOTICES *

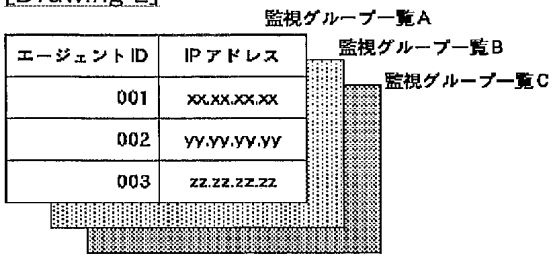
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

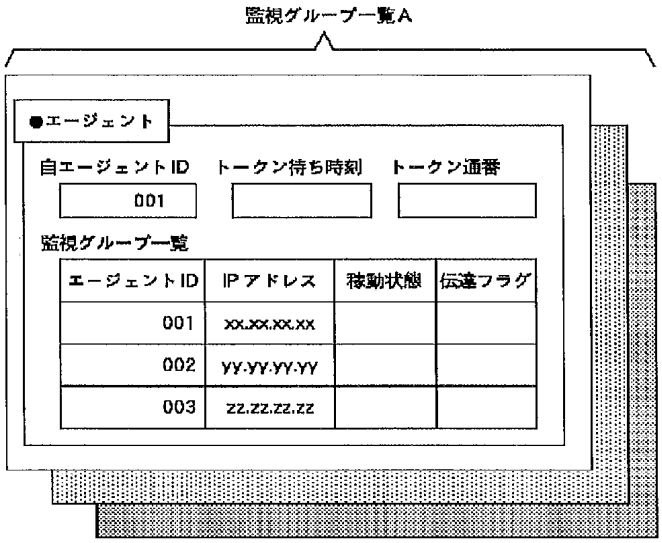
[Drawing 1]



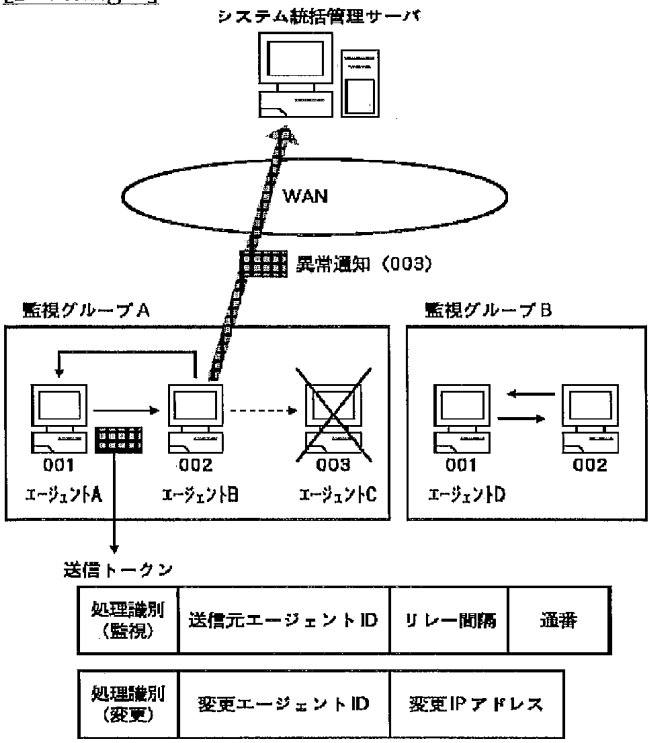
[Drawing 2]



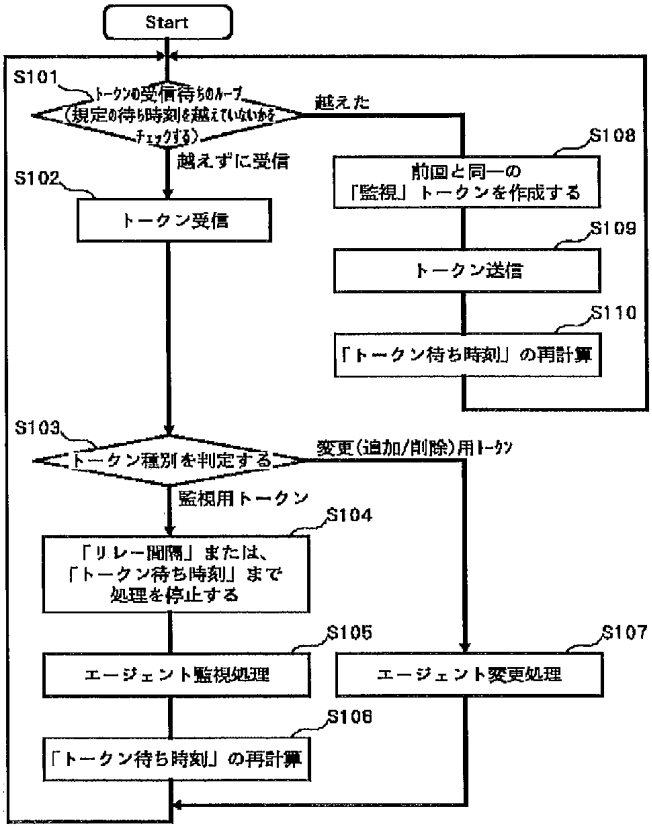
[Drawing 3]



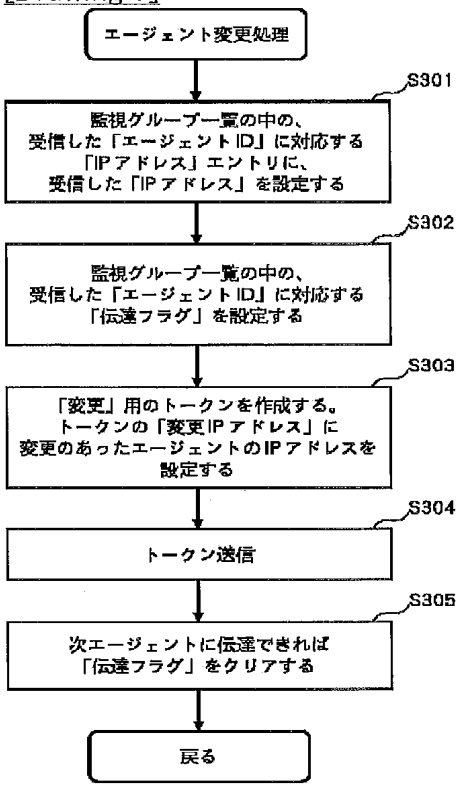
[Drawing 4]



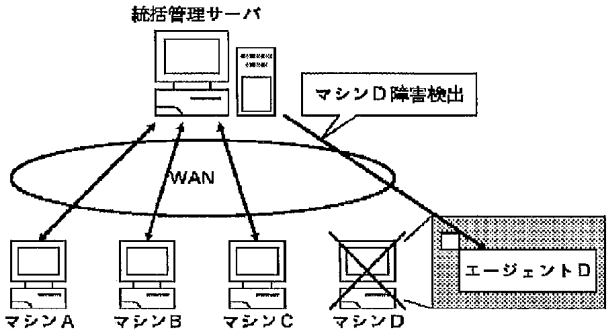
[Drawing 5]



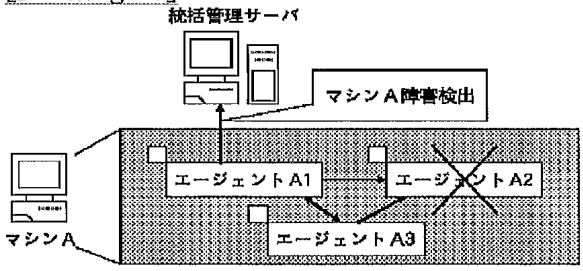
[Drawing 7]



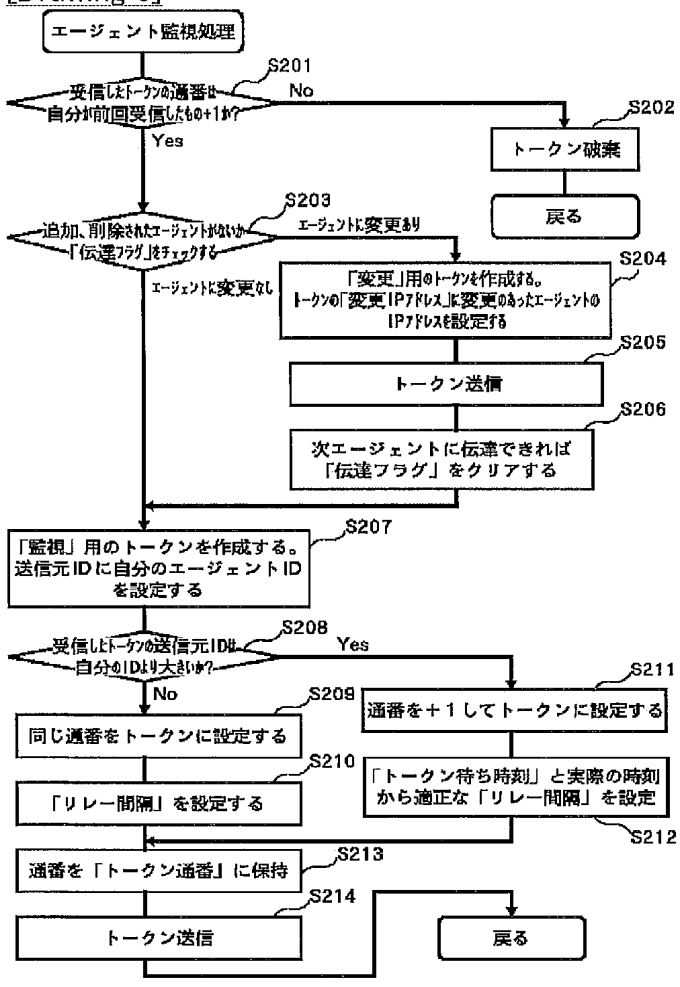
[Drawing 9]



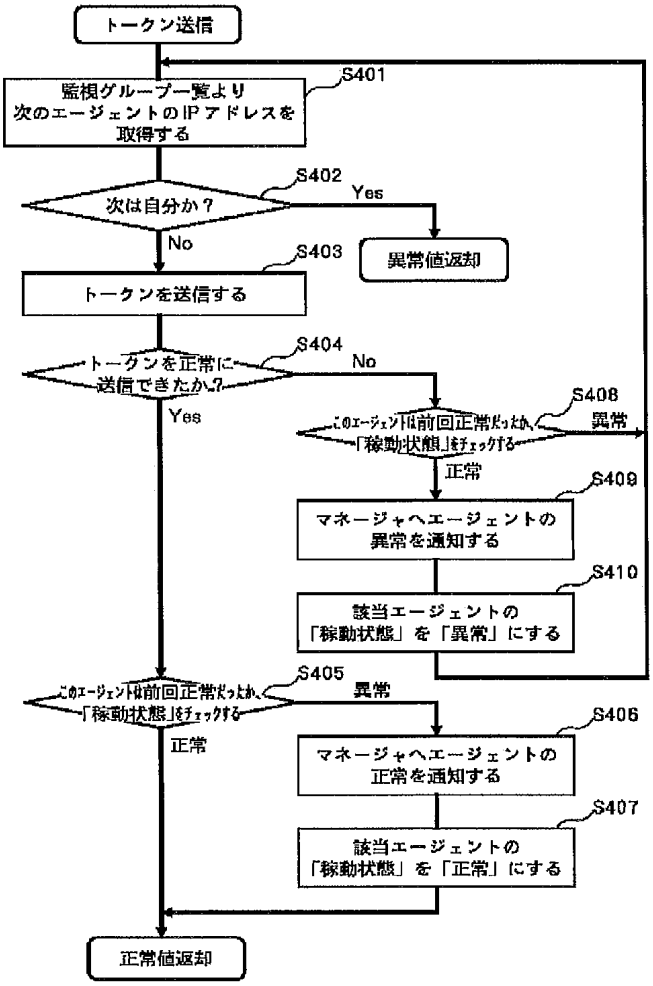
[Drawing 10]



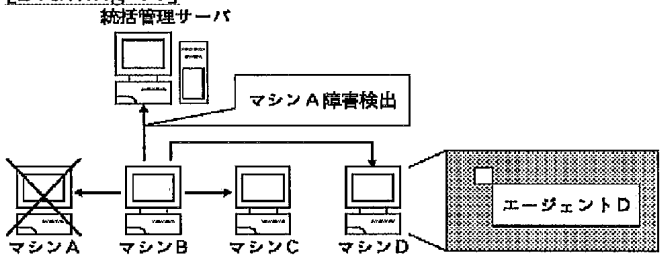
[Drawing 6]



[Drawing 8]



[Drawing 11]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－148539
（P2000－148539A）
(43)公開日　平成12年５月30日(2000.5.30)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０６Ｆ　11/30		Ｇ０６Ｆ　11/30	Ｆ	５Ｂ０４２
			Ｅ	５Ｂ０４５
15/177	６７８	15/177	６７８Ａ	

審査請求　未請求　請求項の数18　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－313729

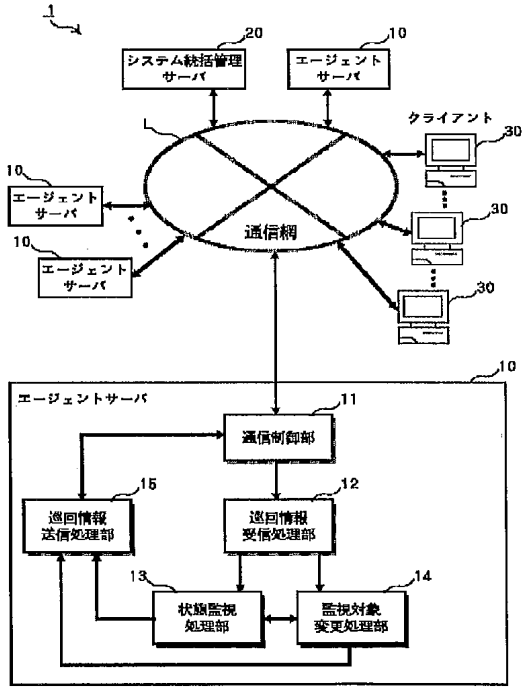
(22)出願日　平成10年11月４日(1998.11.4)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　渡辺　伸一
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

Ｆターム(参考)　5B042 GA12 GB09 GC17 GC19 JJ04
JJ15 JJ17 JJ30 KK11 KK13
KK14
5B045 BB47 BB58 JJ04

(54)【発明の名称】　障害検知方法、コンピュータシステム及び構成装置、記録媒体

(57)【要約】
【課題】　分散システムにおける効率的な障害発生の検知が可能となるコンピュータシステム及び構成装置を提供する。
【解決手段】　エージェントサーバ１０は、巡回情報受信処理部１２において受信トークンの種別を判定し、該判定結果及びエージェント管理情報に基づいて状態監視処理部１３または監視対象変更処理部により対応する送信トークンが生成される。生成された送信トークンは、巡回情報送信処理部１５と共動して次回の送信対象となる他のエージェントサーバ１０に対して送信される。巡回情報送信処理部１５は、該送信結果に基づいて送信先のエージェントサーバ１０における障害発生を検知してエージェント管理情報を更新するとともに、通信制御部１１を介してシステム統括管理サーバ２０に対して該障害発生を通知する。



1

【特許請求の範囲】

【請求項１】　双方向通信可能な環境に分散配置された複数のコンピュータ装置における障害発生の有無を検知する方法であって、

各コンピュータ装置が、

自己以外の他のコンピュータ装置から送出される巡回情報を受領するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて次回の送出対象となる他のコンピュータ装置に対する巡回情報を生成する過程と、

生成された巡回情報を前記次回の送出対象となる他のコンピュータ装置に対して送出するとともに、該送出結果に基づいて送出先のコンピュータ装置における障害の有無を監視して障害発生を検知する過程とを少なくともこの順に実行し、

前記巡回情報を分散配置されたすべてのコンピュータ装置に対して巡回的に波及させ、特定のコンピュータ装置における障害発生の有無をコンピュータ装置間で相互監視することを特徴とする、障害検知方法。

【請求項２】　前記巡回情報は、監視用巡回情報または監視対象変更用巡回情報のいずれかにより形成される情報であり、

前記監視用巡回情報は、送出元のコンピュータ装置に関する識別情報、該巡回情報の送出時間を抑制するためのリレー間隔、及び該巡回情報の整合性を維持するための通番を含んで形成される情報であり、

前記監視対象変更用巡回情報は、前記双方向通信可能な環境に対して追加または削除される監視対象のコンピュータ装置に関する識別情報を含んで形成される情報であることを特徴とする、

請求項１記載の障害検知方法。

【請求項３】　前記監視対象変更用巡回情報は、特定のコンピュータ装置の追加または削除による前記双方向通信可能な環境に対する変更情報を、分散配置されたすべてのコンピュータ装置に対して波及させるための情報であることを特徴とする、

請求項１または２記載の障害検知方法。

【請求項４】　前記巡回履歴情報は、自己のコンピュータ装置に関する識別情報、自己のコンピュータ装置における前記巡回情報の現時点までの到達状態を表す情報、現時点における他のコンピュータ装置に関する稼働状態を表す情報、及び前記監視対象変更用巡回情報の波及状態を表す情報を含んで形成される情報であり、前記コンピュータ装置毎に更新可能に保持されることを特徴とする、

請求項１乃至３のいずれかの項記載の障害検知方法。

【請求項５】　前記巡回履歴情報は、前記巡回情報の伝達順序を特定するための、前記分散配置の形態に基づいて予めグループ化された、自己のコンピュータ装置が属するグループにおける監視対象となるすべてのコンピュータ装置に関する情報を含んで形成されるものであることを特徴とする、

2

請求項１乃至４のいずれかの項記載の障害検知方法。

【請求項６】　双方向通信可能な環境を統括的に管理する第１コンピュータ装置と複数の第２コンピュータ装置とを各々接続して成り、

個々の第２コンピュータ装置は、

自己以外の他の第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第２コンピュータ装置に対する送信巡回情報を生成する巡回情報生成手段と、

生成された送信巡回情報を前記次回の送信対象となる他の第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第２コンピュータ装置における障害の有無を監視して障害発生を検知する障害検知手段と、

検知された障害発生に関する情報を前記第１コンピュータ装置に対して通知する障害通知手段とを備え、

前記障害検知手段が障害発生を検知する毎に前記第１コンピュータ装置に対して通知することを特徴とする、

障害検知機能付きコンピュータシステム。

【請求項７】　前記巡回情報生成手段は、受信した前記巡回情報の種別に基づいて監視用または監視対象変更用のいずれかの前記送信巡回情報を生成するように構成されていることを特徴とする、

請求項６記載のコンピュータシステム。

【請求項８】　前記巡回情報生成手段は、前記巡回履歴情報に基づいて、前記自己以外の他の第２コンピュータ装置からの前記巡回情報が予め設定された待ち時間を超過した場合に、自己の第２コンピュータ装置から前回送信された送信巡回情報と同一の監視用送信巡回情報を生成するように構成されていることを特徴とする、

請求項６または７記載のコンピュータシステム。

【請求項９】　前記巡回情報生成手段は、受信した前記巡回情報が監視対象変更用の巡回情報である場合に、当該巡回情報に基づいて前記双方向通信可能な環境に対して追加または削除される他の第２コンピュータ装置に関する情報を前記巡回履歴情報に反映させて更新するように構成されていることを特徴とする、請求項６または７記載のコンピュータシステム。

【請求項１０】　前記障害検知手段は、前記巡回履歴情報に基づいて前記次回の送信対象となる他の第２コンピュータ装置を特定して前記送信巡回情報を送信するとともに、該送信先の第２コンピュータ装置からの所定の送達確認情報と前記巡回履歴情報とに基づいて、該送信先の第２コンピュータ装置における稼働状態を「正常」または「異常」のいずれかを判定することにより障害発生の有無を検知するように構成されていることを特徴とする、

請求項６記載のコンピュータシステム。

【請求項１１】　前記障害検知手段は、前記送信先の第２コンピュータ装置における稼働状態が「異常」と判定された場合に、前記巡回履歴情報に基づいて、さらに次回の送信対象となる他の第２コンピュータ装置を特定して当該送信巡回情報を継続して送信するように構成されていることを特徴とする、
請求項１０記載のコンピュータシステム。
【請求項１２】　前記障害通知手段は、前記送信先の第２コンピュータ装置における稼働状態が「正常」と判定され、且つ、前記巡回履歴情報における当該送信先の第２コンピュータ装置の稼働状態が「異常」の場合には、前記第１コンピュータ装置に対して当該送信先の第２コンピュータ装置の復旧を表す「正常」に関する情報を通知するように構成されていることを特徴とする、
請求項１０記載のコンピュータシステム。
【請求項１３】　前記障害検知手段は、前記送信先の第２コンピュータ装置に対する前記送信巡回情報の送信完了を契機に、該送信結果及び障害検知結果を反映させて前記巡回履歴情報を更新するように構成されていることを特徴とする、
請求項１２記載のコンピュータシステム。
【請求項１４】　前記第２コンピュータ装置は、所定のトークンパッシングに基づいたトークンによる巡回情報を、前記巡回履歴情報に基づいて、前記双方向通信可能な環境において分散配置された対応する他のすべての前記第２コンピュータ装置に対して巡回させるように構成されていることを特徴とする、
請求項６乃至１３のいずれかの項記載のコンピュータシステム。
【請求項１５】　双方向通信可能な環境において情報取得要求元となる複数の第１コンピュータ装置、前記第１コンピュータ装置に対して情報提供を行う複数の第２コンピュータ装置、及び前記双方向通信可能な環境を統括的に管理する第３コンピュータ装置を各々接続して成り、
前記第１及び第２コンピュータ装置は、
自己以外の他の第１または第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第１または第２コンピュータ装置に対する送信巡回情報を生成する巡回情報生成手段と、
生成された送信巡回情報を前記次回の送信対象となる他の第１または第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第１または第２コンピュータ装置における障害の有無を監視して障害発生を検知する障害検知手段と、
検知された障害発生に関する情報を前記第３コンピュータ装置に対して通知する障害通知手段とを備え、
前記障害検知手段が障害発生を検知する毎に前記第３コンピュータ装置に対して通知することを特徴とする、

障害検知機能付きコンピュータシステム。
【請求項１６】　前記双方向通信可能な環境は、複数の局所的なネットワーク環境をその内部に含んで構築された、アウトソーシング可能な所定のＩＳＤＮを含む広域ネットワーク環境であることを特徴とする、
請求項６または１５記載のコンピュータシステム。
【請求項１７】　既定のＴＣＰ／ＩＰに準拠した通信プロトコルに基づいて構成されていることを特徴とする、
請求項１６記載のコンピュータシステム。
【請求項１８】　双方向通信可能な環境を統括的に管理する第１コンピュータ装置と複数の第２コンピュータ装置とに各々接続され、特定の前記第２コンピュータ装置に読み取られて当該コンピュータ装置を他の前記第２コンピュータ装置に対する稼働状態監視装置として機能させるプログラムコードを記録した記録媒体であって、
前記プログラムコードが、少なくとも、
自己以外の他の第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第２コンピュータ装置に対する送信巡回情報を生成する処理、
生成された送信巡回情報を前記次回の送信対象となる他の第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第２コンピュータ装置における障害の有無を監視して障害発生を検知する処理、
検知された障害発生に関する情報を前記第１コンピュータ装置に対して通知する処理、
を前記第２コンピュータ装置に実行させるものであることを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、システム管理、障害検知技術に係り、より詳しくは、分散システムのネットワーク環境においてデータ通信に係るトラフィックを低減させてコンピュータ装置における障害発生を効率的に検知する手法に関する。
【０００２】
【従来の技術】近年、インタネット等の通信網に代表される大規模且つ高速なネットワーク環境の発展により、利用者に対して多様な形態で情報提供を行うコンピュータシステムの開発が盛んである。これらのコンピュータシステムでは、障害発生に伴うシステム全体の効率低下や、システムへの不正侵入者に対する機密保護等を考慮した、高信頼のシステム構築及びシステム運用管理が望まれている。
【０００３】また、このようなコンピュータシステムでは、例えば、特有な処理の実行及び情報の保持等を担当する複数のコンピュータ装置をネットワーク上に分散して配置し、システム全体における処理効率の向上を図る分散システムが知られている。この分散システムでは、

通常、クライアント・サーバシステム型の通信形態が採用されており、利用者は、クライアント側となるコンピュータ装置からアクセス用インタフェースを使用して、サーバにアクセスし、所望の電子化情報を取得するようになっている。

【０００４】分散システムにおける構築の一形態として、例えば、ネットワーク環境を複数のＬＡＮ（Local Area Network）を含んだ大規模なＷＡＮ（Wide Area Network）環境により構築して、WWW（World Wide Web）サーバ、ＤＮＳ（Domain Name System）、Ｐｒｏｘｙサーバ等の特有な処理を担当する各サーバを該ＷＡＮ上に分散配置させるとともに、システム全体を統括的に管理する統括管理サーバにより一元的な運用管理を行うシステム管理手法が知られている。

【０００５】このようなシステム管理手法では、統括管理サーバが、後述する各エージェントの起動を確認することにより、エージェントの稼働状態を監視して障害発生の検知を行うものである。具体的には、監視対象となるサーバ等の複数のコンピュータ装置に対する統括的な稼働状態の監視を行う監視マネージャ的な統括管理サーバからの集中管理を行うために、分散配置された各サーバマシン等において、監視エージェント（以下、単に「エージェント」と記す）と呼ばれる監視アプリケーションを常駐させるものである。エージェントには、通常、「イベントドリブン方式」が採用されており、エージェントにおいて障害発生が検出された場合にのみ、統括管理サーバへその旨が通知されるようになっている。

【０００６】このイベントドリブン方式では、エージェントと統括管理サーバ間のトラフィック及び統括管理サーバのリソース使用率を軽減させるメリットがあるものの、統括管理サーバにおいて特定のエージェントからの通知がない場合に、当該エージェントが正常に稼働中でありながら通知がないのか、或いは当該エージェントが停止していて通知がないのかが統括管理サーバからは判断できない。

【０００７】このような問題を解決するため、イベントドリブン方式でありながら、且つ統括管理サーバにおいて複数のエージェントの稼働状態をリアルタイムに知ることが可能なように、いくつかの障害検知手法が提案されている。以下、従来の障害検知手法について図面を参照してその概略を説明する。なお、統括管理サーバとエージェント間のデータ通信は、ネットワーク経由のリモートアクセスによるものとする。

【０００８】（１）統括管理サーバからのポーリング

図９は、従来型の分散システムにおける一実施形態を表す図である。統括管理サーバは、各エージェントの起動を確認するために、統括管理サーバ側から監視対象となる各マシンのエージェントに対して周期的に起動確認の問い合わせ、即ちポーリングを行うとともに、各エージェントは、該問い合わせに対して確認を返す。エージェントに異常等が発生した場合、統括管理サーバへの確認が返らないため、統括管理サーバ側では、該確認不能を契機に当該エージェントにおける障害検知が可能となる。

【０００９】（２）監視対象マシン内でのプロセス相互監視

図１０は、従来型のコンピュータ装置におけるプロセス間の相互監視を表す図である。この図では、分散システムを構成する特定のコンピュータ装置（以下、「マシン」と称する）におけるエージェントプロセス間の相互監視を表している。本手法は、監視対象となる各マシンの内部で各々複数のエージェントプロセスを起動し、各エージェントプロセスが互いに起動しているか否かを監視し合うことによってエージェントプロセスのダウン等の障害を検知するものである。例えば、特定のエージェントプロセスがダウンした場合に、他のエージェントプロセスがダウンしたエージェントプロセスを再起動可能に構成されているため、エージェントプロセスがダウンし続ける状態の防止が可能となる。また、特定のエージェントプロセスのダウン検知と同時に、他のエージェントプロセスから該障害発生が統括管理サーバへ通知されるため、統括管理サーバ側からのマシンに対する障害検知が可能となる。

【００１０】（３）サブ統括管理サーバ設置

図１１は、従来型の分散システムにおける実施の一形態を表す図である。通常の分散システムでは、監視対象マシンは同一ＬＡＮ内において複数台設置されることが多いことから、エージェント自身も複数存在する。そこで本手法は、複数の監視対象マシンにおける特定のエージェントが、ＬＡＮ内におけるサブ統括管理サーバとしての機能を果たすように構成するものである。サブ統括管理サーバとして機能するエージェントは、他のエージェントに対して一定時間毎に問い合わせを行い、特定のエージェントからの確認が返らない場合には、当該エージェントの障害発生を統括管理サーバに対して通知する。統括管理サーバでは、該通知を契機に対応するエージェントに係る監視対象マシンの障害を検知する。

【００１１】

【発明が解決しようとする課題】ところで、上述の分散システムにおける障害検知手法では、以下に示すような問題があった。

（１）統括管理サーバからのポーリング

エージェント数の増加に伴ってポーリングに係る通信量も増加するために、ネットワークにおける負荷が増大する。この場合、ポーリングの間隔を長くすることで多少の解決は行えるが、分散システムにおけるリアルタイム性が損なわれてしまう。また、統括管理サーバとエージェント間のネットワークがＩＳＤＮ（Integrated Services Digital Network）の様なＷＡＮの場合、ポーリング毎に課金されてしまうことから、経済的効率を考慮し

たシステム構築の必要性がある。

【００１２】（２）監視対象マシン内でのプロセス交互監視

監視対象となる同一マシン内においてエージェントのダウン防止は可能となるものの、当該マシン自体がダウンした場合についての対処が行えない。

【００１３】（３）サブ統括管理サーバ設置

サブ統括管理サーバとして機能するエージェントがダウンした場合、当該エージェントが監視対象としていた他のエージェントの稼働状態が把握不能となる。これに対処してサブ統括管理サーバのエージェントを複数設置した場合、ネットワーク負荷が増大してしまいそのトレードオフの判断が難しくなる。また、サブ統括管理サーバがどのエージェントを監視するかという情報も必要となることからサブ統括管理サーバ数の増加に伴って必要となる情報伝達量も増大する。

【００１４】このような問題は、障害発生の検知に関して、統括管理サーバとエージェント間の通信トラフィック及びリソースの使用効率を考慮した分散システムを構築できれば解決されるものである。

【００１５】そこで本発明の課題は、分散システムにおける効率的な障害発生の検知が可能となる障害検知方法を提供することにある。本発明の他の課題は、上記障害検知方法の実施に適したコンピュータシステムとその構成装置を提供することにある。また、本発明の他の課題は、上記障害検知方法及びコンピュータシステム等を汎用のコンピュータ装置で実現するための記録媒体を提供することにある。

【００１６】

【課題を解決するための手段】上記課題を解決する本発明の障害検知方法は、双方向通信可能な環境に分散配置された複数のコンピュータ装置における障害発生の有無を検知する方法であって、各コンピュータ装置が、自己以外の他のコンピュータ装置から送出される巡回情報を受領するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて次回の送出対象となる他のコンピュータ装置に対する巡回情報を生成する過程と、生成された巡回情報を前記次回の送出対象となる他のコンピュータ装置に対して送出するとともに、該送出結果に基づいて送出先のコンピュータ装置における障害の有無を監視して障害発生を検知する過程とを少なくともこの順に実行し、前記巡回情報を分散配置されたすべてのコンピュータ装置に対して巡回的に波及させ、特定のコンピュータ装置における障害発生の有無をコンピュータ装置間で相互監視することを特徴とする。

【００１７】上述の各情報の内容は以下のとおりである。

（１）巡回情報：監視用巡回情報または監視対象変更用巡回情報のいずれかにより形成される情報。

（２）監視用巡回情報：送出元のコンピュータ装置に関する識別情報、上記巡回情報の送出時間を抑制するためのリレー間隔、及びその巡回情報の整合性を維持するための通番を含んで形成される情報。

（３）監視対象変更用巡回情報：前記双方向通信可能な環境に対して追加または削除される監視対象のコンピュータ装置に関する識別情報を含んで形成される情報。この監視対象変更用巡回情報は、特定のコンピュータ装置の追加または削除による前記双方向通信可能な環境に対する変更情報を、分散配置されたすべてのコンピュータ装置に対して波及させるための情報である。

（４）巡回履歴情報：自己のコンピュータ装置に関する識別情報、自己のコンピュータ装置における前記巡回情報の現時点までの到達状態を表す情報、現時点における他のコンピュータ装置に関する稼働状態を表す情報、及び前記監視対象変更用巡回情報の波及状態を表す情報を含んで形成される情報であり、前記コンピュータ装置毎に更新可能に保持されるものである。この巡回履歴情報は、前記巡回情報の伝達順序を特定するための、前記分散配置の形態に基づいて予めグループ化された、自己のコンピュータ装置が属するグループにおける監視対象となるすべてのコンピュータ装置に関する情報を含んで形成されるものであっても良い。

【００１８】上記他の課題を解決する本発明のコンピュータシステムは、双方向通信可能な環境を統括的に管理する第１コンピュータ装置と複数の第２コンピュータ装置とを各々接続して成り、個々の第２コンピュータ装置が、自己以外の他の第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第２コンピュータ装置に対する送信巡回情報を生成する巡回情報生成手段と、生成された送信巡回情報を前記次回の送信対象となる他の第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第２コンピュータ装置における障害の有無を監視して障害発生を検知する障害検知手段と、検知された障害発生に関する情報を前記第１コンピュータ装置に対して通知する障害通知手段とを備え、前記障害検知手段が障害発生を検知する毎に前記第１コンピュータ装置に対して通知することを特徴とする、障害検知機能付きコンピュータシステムである。

【００１９】前記巡回情報生成手段は、例えば、受信した前記巡回情報の種別に基づいて監視用または監視対象変更用のいずれかの前記送信巡回情報を生成するように構成される。あるいは、前記巡回履歴情報に基づいて、前記自己以外の他の第２コンピュータ装置からの前記巡回情報が予め設定された待ち時間を超過した場合に、自己の第２コンピュータ装置から前回送信された送信巡回情報と同一の監視用送信巡回情報を生成するように構成される。あるいは、受信した前記巡回情報が監視対象変更用の巡回情報である場合に、当該巡回情報に基づいて

前記双方向通信可能な環境に対して追加または削除される他の第２コンピュータ装置に関する情報を前記巡回履歴情報に反映させて更新するように構成される。

【００２０】前記障害検知手段は、前記巡回履歴情報に基づいて前記次回の送信対象となる他の第２コンピュータ装置を特定して前記送信巡回情報を送信するとともに、該送信先の第２コンピュータ装置からの所定の送達確認情報と前記巡回履歴情報とに基づいて、該送信先の第２コンピュータ装置における稼働状態を「正常」または「異常」のいずれかを判定することにより障害発生の有無を検知するように構成される。この障害検知手段において、稼働状態が「異常」と判定された場合は、前記巡回履歴情報に基づいて、さらに次回の送信対象となる他の第２コンピュータ装置を特定して当該送信巡回情報を継続して送信する。また、稼働状態が「正常」と判定され、且つ、前記巡回履歴情報における当該送信先の第２コンピュータ装置の稼働状態が「異常」の場合には、前記第１コンピュータ装置に対して当該送信先の第２コンピュータ装置の復旧を表す「正常」に関する情報を通知する。なお、前記送信先の第２コンピュータ装置に対する前記送信巡回情報の送信完了を契機に、該送信結果及び障害検知結果を反映させて前記巡回履歴情報を更新する。

【００２１】前記第２コンピュータ装置は、例えば、所定のトークンパッシングに基づいたトークンによる巡回情報を、前記巡回履歴情報に基づいて、前記双方向通信可能な環境において分散配置された対応する他のすべての前記第２コンピュータ装置に対して巡回させるように構成されたものである。

【００２２】本発明の他のコンピュータシステムは、双方向通信可能な環境において情報取得要求元となる複数の第１コンピュータ装置、前記第１コンピュータ装置に対して情報提供を行う複数の第２コンピュータ装置、及び前記双方向通信可能な環境を統括的に管理する第３コンピュータ装置を各々接続して成り、前記第１及び第２コンピュータ装置が、自己以外の他の第１または第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第１または第２コンピュータ装置に対する送信巡回情報を生成する巡回情報生成手段と、生成された送信巡回情報を前記次回の送信対象となる他の第１または第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第１または第２コンピュータ装置における障害の有無を監視して障害発生を検知する障害検知手段と、検知された障害発生に関する情報を前記第３コンピュータ装置に対して通知する障害通知手段とを備え、前記障害検知手段が障害発生を検知する毎に前記第３コンピュータ装置に対して通知することを特徴とする、障害検知機能付きコンピュータシステムである。

【００２３】上記他の課題を解決する本発明の記録媒体は、双方向通信可能な環境を統括的に管理する第１コンピュータ装置と複数の第２コンピュータ装置とに各々接続され、特定の前記第２コンピュータ装置に読み取られて当該コンピュータ装置を他の前記第２コンピュータ装置に対する稼働状態監視装置として機能させるプログラムコードを記録した記録媒体であって、前記プログラムコードが、少なくとも、自己以外の他の第２コンピュータ装置から送信される巡回情報を受信するとともに、当該巡回情報と予め保持された巡回履歴情報とに基づいて、次回の送信対象となる他の第２コンピュータ装置に対する送信巡回情報を生成する処理、生成された送信巡回情報を前記次回の送信対象となる他の第２コンピュータ装置に対して送信するとともに、該送信結果に基づいて送信先の第２コンピュータ装置における障害の有無を監視して障害発生を検知する処理、検知された障害発生に関する情報を前記第１コンピュータ装置に対して通知する処理、を前記第２コンピュータ装置に実行させるものである。

【００２４】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。

（第１実施形態）図１は、本発明を、情報提供を行うコンピュータシステムに適用した場合の実施の形態を表す機能ブロック図である。このコンピュータシステム１は、複数のエージェントサーバ１０、システム全体の統括管理を行うシステム統括管理サーバ２０、及び複数のクライアント３０を分散して配備し、通信網Ｌを介して各々双方向通信可能に接続されて構成される。この場合の通信網Ｌは、例えば、複数のＬＡＮ等の局所的なネットワーク環境をその内部に含んで構築された、アウトソーシング可能なＩＳＤＮ等を含むＷＡＮによる広域ネットワーク環境である。

【００２５】エージェントサーバ１０は、当該サーバを構成するコンピュータ装置が保有した固有のアプリケーション及び情報に関するサービスを複数のクライアント３０に対して提供する業務サーバであるとともに、複数のエージェントサーバ１０相互間において稼働状態の監視を行う所謂、稼働状態監視装置として機能するものである。複数のエージェントサーバ１０における個々のサーバ機能は、例えば、ＤＮＳ、Ｐｒｏｘｙ、ＷＩＮＳ（Windows Internet Network Service）、データベース管理システム（ＤＢＭＳ）等を提供するように構成される。

【００２６】以下、本実施形態では、エージェントサーバ１０における機能構成について、公知技術により実現されるクライアント３０に対するサーバ機能に関する説明を省略し、複数のエージェントサーバ１０間における稼働状態監視装置としての機能構成について説明する。なお、複数のエージェントサーバ１０間におけるデータ

アクセスは、所定のトークンによるメッセージを予め設定されたノード順序でネットワークを巡回させる、公知のトークンパッシング手法（Token Passing Method）に基づくものとする。

【００２７】システム統括管理サーバ２０は、コンピュータシステム１全体を統括的に管理するサーバであり、複数のエージェントサーバ１０に対する監視マネージャとして位置付けられる。具体的には、特定のエージェントサーバ１０において障害が発生した場合に、他のエージェントサーバ１０からなされる障害発生の通知に即して障害を検知したシステム統括管理サーバ２０は、該障害に関する情報を管理者へ通知を行ったり、記録（ログ）を残したりするように構成される。

【００２８】また、システム統括管理サーバ２０は、図示しない情報保持手段において複数のエージェントサーバ１０に関する監視管理情報を保持するものである。図２に、監視管理情報における構築形態の一例を示す。図中、「エージェントＩＤ」は各エージェントサーバ１０毎に各々付与された識別情報であり、監視管理情報は、「エージェントＩＤ」と対応するエージェントサーバ１０の「ＩＰアドレス」との組から構築されている。この場合、「エージェントＩＤ」は予め設定された監視グループ内で一意に決められるものであり、トークンの伝達順序に用いるために数値であることが望ましい。また、監視グループとは、複数のエージェントサーバ１０間で稼働状態の相互監視を行うためのエージェントサーバの集合であり、ネットワーク的に離れたエージェントサーバ同士が監視し合うことがないように、好ましくは、同一ＬＡＮのようにその分散形態に即した同一サイトやセグメント等に属するエージェントサーバ群として構築すれば良い。このことから、システム統括管理サーバ２０では、すべての監視グループに関する監視管理情報を保有するものとなる。

【００２９】なお、本実施形態におけるコンピュータシステム１は、公知のＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）の通信プロトコルをベースに構成されているものとする。但し、このような例に限定されず、ＵＤＰの通信プロトコルをベースに構成されたものであっても良い。

【００３０】コンピュータ装置により実現される、稼働状態監視装置として機能するエージェントサーバ１０は、自己のＯＳ下で所定のプログラムを読み込んで実行することにより形成される、通信制御部１１、巡回情報受信処理部１２、状態監視処理部１３、監視対象変更処理部１４、及び巡回情報送信処理部１５を具備して構成される。

【００３１】また、エージェントサーバ１０における各機能を形成させる上記プログラムは、通常、当該エージェントサーバ１０を構成するコンピュータ装置の内部或いは外部記憶装置に、上記各機能ブロックを形成可能な任意の記録形態で格納され、随時読み取られて実行されるようになっている。例えば、コンピュータ装置等とは分離可能なＣＤ－ＲＯＭやＦＤ等の可搬性記録媒体、或いは構内ネットワークに接続されたプログラムサーバ等にコンピュータ可読の形態で格納され、使用時に上記コンピュータ装置の内部または外部記憶装置にインストールされて随時実行に供されるものであってもよい。なお、上記機能ブロック１１～１５は、上記プログラム単独による形成、或いはコンピュータ装置に搭載されたオペレーティングシステムとの共動により適宜実現されるものであっても良い。

【００３２】通信制御部１１は、通信網Ｌを介してシステム統括管理サーバ２０及び複数のエージェントサーバ１０とのデータ授受を行うものである。

【００３３】巡回情報受信処理部１２は、稼働状態の監視対象となる複数のエージェントサーバ１０から巡回してなされる応答情報、即ちトークン（以下、受信トークン）を後述するエージェント管理情報に基づいて通信制御部１１を介して受信するとともに、当該受信トークンの種別について「監視用トークン」かまたは「変更用トークン」かを判定するものである。

【００３４】状態監視処理部１３は、巡回情報受信処理部１２における受信トークンが「監視用トークン」の場合に、次回に巡回させるべきエージェントサーバ監視用の送信トークンを後述するエージェント管理情報に基づいて生成するとともに、当該トークンを巡回情報送信処理部１５と共動することにより通信制御部１１を介して送信対象となる他のエージェントサーバ１０に対して送信するものである。

【００３５】監視対象変更処理部１４は、巡回情報受信処理部１２における受信トークンが、監視対象となる特定のエージェントサーバ１０に関する追加または削除を表す「変更用トークン」の場合に、次回に巡回させるべきエージェントサーバ変更用の送信トークンを後述するエージェント管理情報に基づいて生成するとともに、当該トークンを巡回情報送信処理部１５と共動することにより通信制御部１１を介して送信対象となる他のエージェントサーバ１０に対して送信するものである。

【００３６】巡回情報送信処理部１５は、状態監視処理部１３及び監視対象変更処理部１４において各々生成された送信トークンを通信制御部１１を介して送信対象となる他のエージェントサーバ１０に対して送信するとともに、該送信結果と後述するエージェント管理情報とに基づいて当該トークンの送信先エージェントサーバ１０における稼働状態を判定するものである。また、該判定結果を、通信制御部１１を介してシステム統括管理サーバ２０に対して通知するように構成される。具体的には、送信トークンを巡回させるべき送信先エージェントサーバ１０に対して送信不能な場合を、当該エージェントサーバ１０における障害発生として検知する毎に、該

障害検知に関する情報をシステム統括管理サーバ２０に対して通知する。

【００３７】この場合、送信トークンは、障害が検知されたエージェントサーバ１０の次に送信対象となる他のエージェントサーバ１０に対して継続して送信され、障害が検知された同一エージェントサーバ１０に対しては、送信トークンが自己のエージェントサーバ１０に巡回してきた場合に再度送信を行うように構成される。

【００３８】次に、エージェントサーバ１０におけるエージェント管理情報について説明する。エージェントサーバ１０は、図示しない情報管理手段において予め構築されたエージェント管理情報を保持するとともに、当該エージェント管理情報に基づいて上記機能ブロック１１～１５を機能させるものである。

【００３９】図３にエージェント管理情報における構築形態の一例を示す。図中、「エージェントＩＤ」及び「ＩＰアドレス」は、上述のシステム統括管理サーバ２０における監視管理情報に対応するものであり、トークンの伝達順序はこの「エージェントＩＤ」に基づいて決定される。なお、エージェント管理情報において、例えば、欠番となっている「エージェントＩＤ」に対応する「ＩＰアドレス」はゼロクリアするように構築すれば良い。

【００４０】「稼働状態」は、現時点において対応するエージェントサーバ１０が稼働しているか否かを表す情報であり、この「稼働状態」は、すべてのエージェントサーバ１０の稼働状態に関する情報を保持する必要はなく、例えば、過去に自己のエージェントサーバ１０からトークンを伝達したエージェントサーバ１０に関する情報だけがあれば良い。

【００４１】「伝達フラグ」は、特定のエージェントサーバ１０に関する追加や削除等の変更が行われた場合に、当該エージェントサーバ１０のＩＰアドレス等の情報が次回にトークンを巡回させるべきエージェントサーバ１０に伝達したか否かを表す情報である。変更されたエージェントサーバ１０に関する情報は、自己のエージェントサーバ１０に対して送信がなされた他のエージェントサーバ１０からの送信トークンにより巡回的に伝達される。各エージェントサーバ１０は、監視グループを構成するすべてのエージェントサーバ１０に関する「監視グループ一覧」情報を持つ必要があるため、この「伝達フラグ」により最新情報の保持が実現される。一方、「トークン待ち時刻」及び「トークン通番」は、トークンに関する不整合や通信上のエラーを検出するため情報である。

【００４２】このエージェント管理情報は、エージェントサーバ１０の現時点におけるトークンに関する巡回の履歴情報として用いられる。なお、エージェント管理情報におけるデータ構造は、上記構築例に限定することなく例えば、表形式やリスト形式等対応する形態で適宜構築すれば良い。

【００４３】このように、各エージェントサーバ１０は、自己が属する監視グループに関するエージェント管理情報を保持しておけば良く、当該エージェント管理情報とエージェントサーバ１０間を巡回するトークンとにより稼働状態の相互監視、及び特定のエージェントサーバ１０における構成変更情報の自動伝達が実現される。

【００４４】次に、エージェントサーバ１０間を巡回するトークンについて説明する。図４は、エージェントサーバ１０間における稼働状態の監視処理の概要を表す模式図である。本実施形態では、コンピュータシステム１を巡回するトークン、即ち送信トークンは、図示するように２種類の形態でエージェントサーバ１０間を巡回するものである。エージェントサーバ１０における巡回情報受信処理部１２では、送信トークンを受信して、当該トークンに含まれる「処理種別」を表すフラグから当該トークンが通常の「監視用トークン」か、または特定のエージェントサーバ１０に関する追加や削除等の「変更用トークン」かが判定される。

【００４５】「監視用トークン」は、監視用トークンを表すフラグ「処理種別」、「送信元エージェントＩＤ」、トークンの送信処理時間を抑制するための巡回遅延を表す「リレー間隔」、及びトークンの整合性を維持するための「通番」を含んで構成される。この場合の「通番」は監視グループを一巡する毎にその値が増加するように構成され、また、「リレー間隔」は通番が増加する際に、トークンが流れすぎないように、エージェントサーバ１０において、エージェント管理情報の「トークン待ち時刻」と実際の時刻とから一巡する時間を加味して算出された値が付与されるものである。

【００４６】一方、「変更用トークン」は、変更用トークンを表すフラグ「処理種別」、コンピュータシステム１における通信網Ｌに対して追加または削除される「変更エージェントＩＤ」、及び対応する「変更ＩＰアドレス」を含んで構成される。この場合、例えば、「変更ＩＰアドレス」が「０」の場合は対応するエージェントサーバ１０の「削除」、また、それ以外の値の場合には対応するエージェントサーバ１０の「追加」と判定するように構成される。

【００４７】また、この図では、監視グループＡにおいてエージェントＩＤ「００３」のエージェントサーバＣに対する送信トークンが送信不能であったため、当該エージェントサーバＣにおける障害が、送信元となるエージェントＩＤ「００２」のエージェントサーバＢにより検知されてシステム統括管理サーバ２０に対する通知がなされていることを表している。

【００４８】次に、本実施形態におけるコンピュータシステム１の具体的な動作について説明する。図５～８は、コンピュータシステム１における処理手順図である。まず、図５に示すエージェントサーバ１０における

概略処理手順について説明する。エージェントサーバ１０の巡回情報受信処理部１２は、エージェント管理情報に基づいてトークンの受信に係る待ち時間を検知する（ステップＳ１０１）。当該待ち時間がエージェント管理情報における「トークン待ち時刻」を超えずに受信された場合（ステップＳ１０１：超えずに受信）、巡回情報受信処理部１２は当該トークンを受信してその種別を判定する（ステップＳ１０２～１０３）。

【００４９】判定された受信トークンの種別が「監視用トークン」の場合には（ステップＳ１０３：監視用トークン）、巡回情報受信処理部１２は、当該トークンにおける「リレー間隔」またはエージェント管理情報における「トークン待ち時間」に基づいて処理を一時停止する（ステップＳ１０４）。この「リレー間隔」で指定された時間待機することにより、通信網Ｌにおけるトラフィックが抑制される。次に、制御権は、巡回情報受信処理部１２から状態監視処理部１３に移されてエージェントサーバ１０間における監視処理が行われる（ステップＳ１０５）。なお、当該監視処理については後述する。

【００５０】当該監視処理が終了後、エージェントサーバ１０は、該監視処理結果に基づいて図示しない情報管理手段により「トークン待ち時間」を再算出してエージェント管理情報を更新するとともに（ステップＳ１０６）、ステップＳ１０１に戻り処理を繰り返す。また、巡回情報受信処理部１２における受信トークンが「変更用トークン」の場合には（ステップＳ１０３：変更用トークン）、制御権は、監視対象変更処理部１４に移されて後述するエージェントサーバ１０に関する変更処理が行われる（ステップＳ１０７）。

【００５１】一方、上記ステップＳ１０１においてトークンが待ち時間を超過して受信された場合には（ステップＳ１０１：超えた）、トークンを保持したままダウン等の障害が発生したエージェントサーバ１０の存在や通信網Ｌが分断された等、何らかの異常が予測できることから、状態監視処理部１３において、前回と同一の監視用の送信トークンを生成する（ステップＳ１０８）。当該トークンは、巡回情報送信処理部１５と共動して自己のエージェントサーバ１０から次回に送信対象となる他のエージェントサーバ１０へ送信され、また、図示しない情報管理手段により「トークン待ち時間」を再算出してエージェント管理情報を更新するとともに（ステップＳ１０９～１１０）、ステップＳ１０１に戻り処理を繰り返す。

【００５２】この場合、次回の送信対象となる他のエージェントサーバ１０とは、エージェント管理情報の監視グループ一覧における「エージェントＩＤ」が、自己のエージェントＩＤの次に大きい値となるエージェントサーバ１０である。自己エージェントＩＤより大きい値となるエージェントＩＤがエージェント管理情報に存在しない場合に、巡回情報送信処理部１５は、例えば、監視グループ内において最小値となるエージェントＩＤに基づいて次回の送信対象エージェントサーバ１０を特定するように構成される。この処理により、再度自己のエージェントサーバ１０へ巡回するトークンから障害の発生源が特定される。なお、トークンの送信処理については後述する。

【００５３】次に、図６に示すエージェントサーバ１０における状態監視処理手順について説明する。状態監視処理部１３は、巡回情報受信処理部１２からの受信トークンに対して、その「通番」が自己エージェントサーバ１０に保持されたエージェント管理情報における「トークン通番」より大きいか否かを判定する（ステップＳ２０１）。具体的には、受信トークンの「通番」とエージェント管理情報における「トークン通番」とを比較して前回受信したものより「１」増分していると判定された場合には（ステップＳ２０１：Yes）、当該トークンにおける「送信元エージェントＩＤ」に基づいてエージェント管理情報の対応する「伝達フラグ」をチェックする（ステップＳ２０３）。一方、受信トークンの「通番」がエージェント管理情報における「トークン通番」より増分していない場合には（ステップＳ２０１：No）、当該受信トークンが二重に巡回していることを表していることから当該受信トークンを破棄する（ステップＳ２０２）。

【００５４】次に、状態監視処理部１３では、エージェント管理情報における「伝達フラグ」のチェックにより、対応するエージェントサーバ１０に変更があると判定された場合には（ステップＳ２０３：エージェントに変更あり）、監視対象変更処理部１４と共動して変更用トークンを生成する（ステップＳ２０４）。具体的には、変更用トークンにおける「変更ＩＰアドレス」を、「伝達フラグ」に対応する変更のあったエージェントサーバ１０のＩＰアドレスにより設定するように構成される。

【００５５】生成された変更用トークンは、巡回情報送信処理部１５により次回の送信対象となる他のエージェントサーバ１０に対して送信され、エージェント管理情報において対応する「伝達フラグ」は、該送信完了を契機に、図示しない情報管理手段によりクリアされる（ステップＳ２０５～２０６）。

【００５６】次に、状態監視処理部１３では、「送信元エージェントＩＤ」に自己のエージェントＩＤを設定して監視用トークンを生成する（ステップＳ２０７）。また、状態監視処理部１３は、受信トークンにおける「送信元エージェントＩＤ」と自己のエージェントＩＤとを比較する。「送信元エージェントＩＤ」が自己のエージェントＩＤ以下の場合には（ステップＳ２０８：No）、エージェント管理情報における「トークン通番」を監視用トークンの「通番」に対して設定するとともに（ステップＳ２０９）、監視用トークンの「リレー間隔」を設

定する（ステップＳ２１０）。

【００５７】一方、「送信元エージェントＩＤ」が自己のエージェントＩＤ以上の場合には（ステップＳ２０８：Yes）、状態監視処理部１３は、エージェント管理情報における「トークン通番」を「１」増分させて監視用トークンの「通番」を設定するとともに（ステップＳ２１１）、エージェント管理情報における「トークン待ち時間」と実際の時刻とに基づいて監視用トークンの「リレー間隔」を設定する（ステップＳ２１２）。

【００５８】また、図示しない情報管理手段では、上記ステップＳ２０８～２１２において監視用トークンに対して設定された「通番」により、エージェント管理情報における「トークン通番」を更新して保持するとともに（ステップＳ２１３）、巡回情報送信処理部１５では、設定された監視用トークンを通信制御部１１を介して送信対象となるエージェントサーバ１０に対して送信する（ステップＳ２１４）。

【００５９】次に、図７に示す特定のエージェントサーバ１０に関する変更処理手順について説明する。特定のエージェントサーバ１０の追加または削除によるコンピュータシステム１に対する変更がなされる場合、当該エージェントサーバが属すべき監視グループに対応する各エージェントサーバ１０が保持するエージェント管理情報に対して該変更を反映させて更新しなければならない。この場合、システム統括管理サーバ２０から各エージェントサーバ１０へ追加や削除等の変更情報を送信するのではなく、変更対象となるエージェントサーバ１０自身が当該変更情報をトークンにより、次回の送信対象となる他のエージェントサーバ１０に対して送信する。この処理により、ダウン等の障害が検知されているエージェントサーバ１０を含めて、当該変更情報は、コンピュータシステム１におけるすべてのエージェントサーバ１０に対してに波及されるものとなる。

【００６０】なお、エージェントサーバ１０追加の場合には、該追加時に予めシステム統括管理サーバ２０から最新の監視グループ一覧及び自己のエージェントＩＤが付与されるものとし、また、エージェントサーバ１０削除の場合には、エージェント管理情報における自己のエージェントＩＤに基づいて変更用トークンが生成されるものとする。

【００６１】まず、監視対象変更処理部１４は、エージェント管理情報の監視グループ一覧において、受信トークンの「エージェントＩＤ」に対応する「ＩＰアドレス」に対して、当該受信トークンのＩＰアドレスを設定する（ステップＳ３０１）。また、監視対象変更処理部１４は、エージェント管理情報において受信トークンの「エージェントＩＤ」に対応する「伝達フラグ」を設定する（ステップＳ３０２）。次に、監視対象変更処理部１４は、変更のあったエージェントサーバ１０のＩＰアドレスを「変更ＩＰアドレス」として設定した「変更用トークン」を生成するとともに（ステップＳ３０３）、巡回情報送信処理部１５と共動して当該トークンを次回の送信対象となるエージェントサーバ１０に対して送信する（ステップＳ３０４）。

【００６２】巡回情報送信処理部１５では、「変更用トークン」の送信完了を契機に、図示しない情報管理手段と共動してエージェント管理情報の対応する「伝達フラグ」をクリアする（ステップＳ３０５）。この場合、例えば、次回の送信対象となる他のエージェントサーバ１０がダウン等していた場合には、さらに次回の送信対象となるエージェントサーバ１０に対して変更用トークンを送信するものの「伝達フラグ」に対するクリアは行わないように構成すれば良い。

【００６３】以上の処理から、追加や削除等の変更対象となるエージェントサーバ１０自身は、変更用トークンを、すべてのエージェントサーバ１０に対して送信することなく、少なくとも１つの送信対象となるエージェントサーバ１０にのみ送信すれば良く、巡回するトークンと「伝達フラグ」とにより、対応する変更情報は、すべてのエージェントサーバ１０に対して確実に波及するものとなる。

【００６４】次に、図８に示すトークンの送信処理手順について説明する。巡回情報送信処理部１５は、エージェント管理情報の監視グループ一覧から次回の送信対象、即ちトークンを次に巡回させるべきエージェントサーバ１０のＩＰアドレスを取得する（ステップＳ４０１）。次回の送信対象が自己のエージェントサーバ１０である場合には（ステップＳ４０２：Yes）、エラーを表す異常値を返却する。一方、次回の送信対象が自己のエージェントサーバ１０以外である場合（ステップＳ４０２：No）、巡回情報送信処理部１５は、通信制御部１１を介して当該エージェントサーバ１０に対してトークンの送信を行う（ステップＳ４０３）。

【００６５】次に、巡回情報送信処理部１５は、通信制御部１１を介してトークンの送信結果を判定する。当該トークンが正常に送信された場合には（ステップＳ４０４：Yes）、エージェント管理情報において当該トークンが送信されたエージェントサーバ１０の「稼働状態」をチェックし、当該「稼働状態」が「正常」の場合には（ステップＳ４０５：正常）、正常値を返却する。

【００６６】一方、当該「稼働状態」が「異常」の場合（ステップＳ４０５：異常）、巡回情報送信処理部１５は、システム統括管理サーバ２０に対して対応するエージェントサーバ１０における「正常」を通知する（ステップＳ４０６）。また、巡回情報送信処理部１５は、図示しない情報管理手段と共動してエージェント管理情報の対応するエージェントサーバ１０に関する「稼働状態」を「正常」に更新する（ステップＳ４０７）。このステップＳ４０５～４０７の処理により、前回までトークンの送信が失敗していたエージェントサーバ１０に関

する、所謂「復旧」の通知がシステム統括管理サーバ２０に対してなされるものとなる。

【００６７】また、上記ステップＳ４０４においてトークンが正常に送信できなかった場合（ステップＳ４０４：No）、巡回情報送信処理部１５は、エージェント管理情報における送信先のエージェントサーバ１０に関する前回の「稼働状態」を判定し、該判定結果が「異常」であった場合には（ステップＳ４０８：異常）、ステップＳ４０１に戻り、さらに次回の送信対象となるエージェントサーバ１０を特定して処理を繰り返す。

【００６８】一方、「稼働状態」が「正常」であった場合（ステップＳ４０８：正常）、巡回情報送信処理部１５は、システム統括管理サーバ２０に対して当該エージェントサーバ１０における障害検知を通知する（ステップＳ４０９）。また、巡回情報送信処理部１５は、図示しない情報管理手段と共動してエージェント管理情報における「稼働状態」を「異常」に更新する（ステップＳ４１０）。

【００６９】上記ステップＳ４０４におけるトークンの送信結果に関する確認手法として、巡回情報送信処理部１５を、例えば、コネクション型の通信であるＴＣＰまたはコネクションレス型のＵＤＰを用いて送信先のエージェントサーバ１０側からなされる送達確認情報を含む応答に基づいてトークンの送信結果を判定するように構成しても良い。

【００７０】このように、本実施形態のコンピュータシステム１では、複数のエージェントサーバ間でトークンを巡回させて各エージェントサーバにおける稼働状態を相互監視するとともに、特定のエージェントサーバにおける障害が検知された場合のみ、他のエージェントサーバ側からシステム統括管理サーバに対して該障害検知が通知されることから、従来手法のようにシステム統括管理サーバからのポーリングを行うことなく、ネットワーク環境における通信トラフィックが低減できる。

【００７１】また、エージェントサーバ相互間で巡回するトークンに基づいて稼働状態を監視し合うことから、各エージェントサーバの起動状態をほぼリアルタイムで確実に把握可能となるとともに、例えば、エージェントサーバ装置自体のダウンや、エージェントサーバにおけるエージェントプロセスのダウン等を障害発生として検出することができる。

【００７２】また、ネットワーク環境におけるすべてのエージェントサーバが同一の立場にあるため、従来手法と比較して稼働状態の監視に係るトラフィックが集中することなく負荷分散が可能となる。

【００７３】また、エージェントサーバにおいて障害が検知された時点にのみシステム統括管理サーバに対して通知されるため、システム統括管理サーバとエージェントサーバ間のネットワーク負荷及びリソースの使用率が著しく軽減される。

【００７４】また、例えば、ＷＡＮを経由した分散システムにおいて、アウトソーシングを実施している場合に、ネットワークへの常時接続が不要となるとともに、必要最低限の通信でエージェントサーバにおける稼働状態をシステム統括管理サーバへ通知可能なことから、通信コストが削減され経済効率が大幅に向上する。

【００７５】また、監視対象となる特定のエージェントサーバに関する追加や削除等の変更情報を、当該エージェントサーバ自身がトークンにより他のエージェントサーバ群に対して巡回させることから、システム統括管理サーバが関与することなくネットワーク環境に当該変更情報を波及させることが可能となる。

【００７６】さらに、特定のエージェントサーバにおいてダウン等の障害が発生していた場合であっても、システム統括管理サーバは関与することなく、巡回するトークンに基づいて他のエージェントサーバ群に対する自動的な情報の伝達が可能となる。このように、本実施形態のコンピュータシステム１によれば、システム全体における信頼性及び運用管理に係る処理効率が大幅に向上する。

【００７７】（第２実施形態）本発明は、例えば、クライアント・サーバシステムにおける複数のクライアントに対して適用させて構成することも可能である。この場合のクライアントは、少なくとも、上記コンピュータシステム１におけるエージェントサーバ１０と同一の機能ブロックである、巡回情報受信処理部１２、状態監視処理部１３、監視対象変更処理部１４、及び巡回情報送信処理部１５を具備して構成される。

【００７８】このクライアントがエージェントサーバ１０と相違する点は、例えば、クライアントに検知した障害発生に関する情報を提示するための表示装置を具備する点であり、クライアントに具備されるディスプレイ装置等の出力装置に対してメッセージ等の出力を行うようにクライアントを構成させる。また、通信制御部１１に相当する処理は、クライアント自体に具備される通信制御の機能を使用することにより代替が可能となる。

【００７９】第１実施形態におけるエージェントサーバ１０は、上述のように、複数のエージェントサーバ間で稼働状態の相互監視を行うものであり、コンピュータシステム１におけるシステムの階層的な観点からは、すべてのエージェントサーバ１０は同位レベルとして位置付けられている。このことから、第２実施形態では、例えば、複数のクライアントを、エージェントサーバ１０と同位レベルのコンピュータ装置として各々機能させように、上記機能ブロック１２～１５を組み込んで具備させ、クライアントを構成することにより上記コンピュータシステム１におけるエージェントサーバ１０と同等の効果を得ることが可能となる。

【００８０】本実施形態のクライアントを用いて上記コンピュータシステム１を構築した場合には、上記システ

ム統括管理サーバ２０以外のすべてのコンピュータ装置が同位レベルとなり、複数のクライアント間、複数のエージェントサーバ１０間、及びクライアント～エージェントサーバ１０間における稼働状態の相互監視が可能となる。

【００８１】

【発明の効果】以上の説明から明らかなように、本発明によれば、分散型のコンピュータシステムにおける効率的な障害発生の検知が可能となるという特有の効果がある。また、本発明のコンピュータシステムによれば、分散システムを構成するコンピュータ装置間で稼働状態の相互監視ができることから、信頼性及び処理効率の高いシステム運用管理環境が実現可能となる効果がある。

【図面の簡単な説明】

【図１】本発明のコンピュータシステムの一実施形態を表す機能ブロック図。

【図２】監視管理情報における構築形態の一例。

【図３】エージェント管理情報における構築形態の一例。

【図４】本実施形態の監視処理の概要を表す模式図。

【図５】本実施形態のエージェントサーバにおける処理手順図。

【図６】状態監視処理における処理手順図。

【図７】エージェント変更処理における処理手順図。

【図８】トークン送信処理における処理手順図。

【図９】従来型の分散システムにおける一実施形態を表す図。

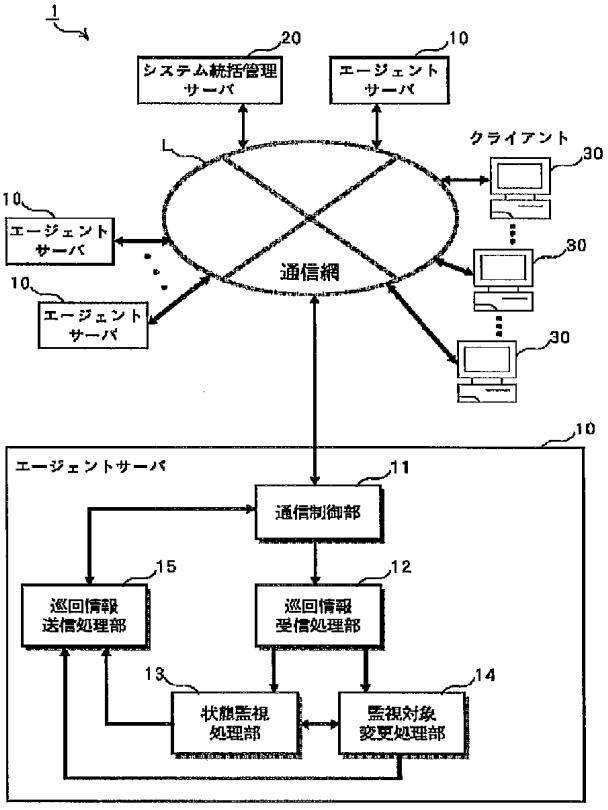
【図１０】従来型のコンピュータ装置におけるプロセス間の相互監視を表す図。

【図１１】従来型の分散システムにおける一実施形態を表す図。

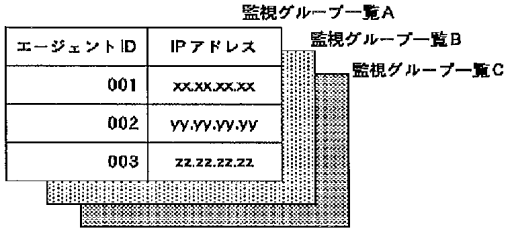
【符号の説明】

１　コンピュータシステム
１０　エージェントサーバ
１１　通信制御部
１２　巡回情報受信処理部
１３　状態監視処理部
１４　監視対象変更処理部
１５　巡回情報送信処理部
２０　システム統括管理サーバ
３０　クライアント
Ｌ　通信網

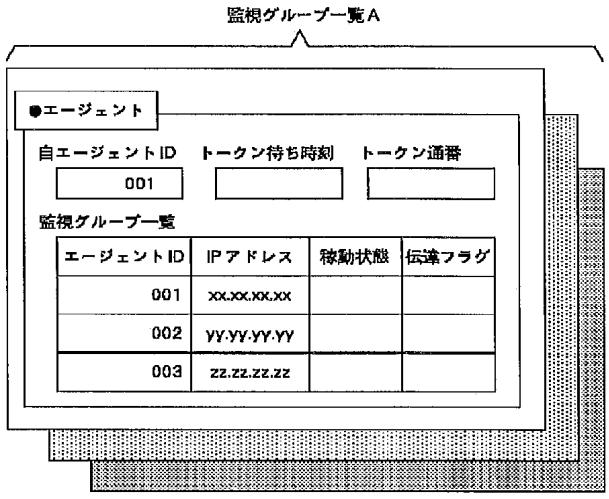
【図１】



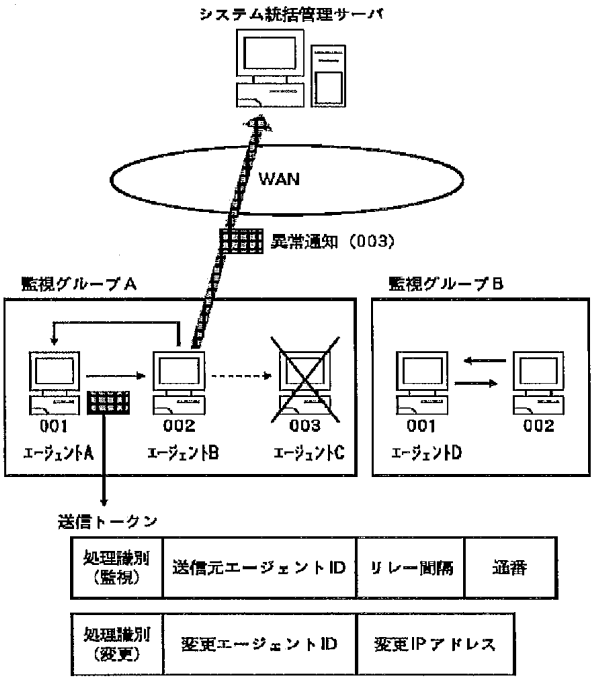
【図２】



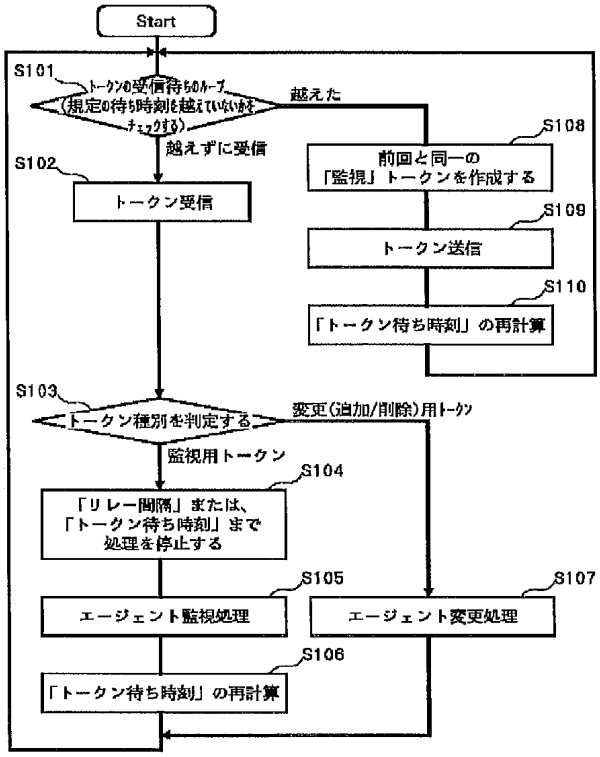
【図３】



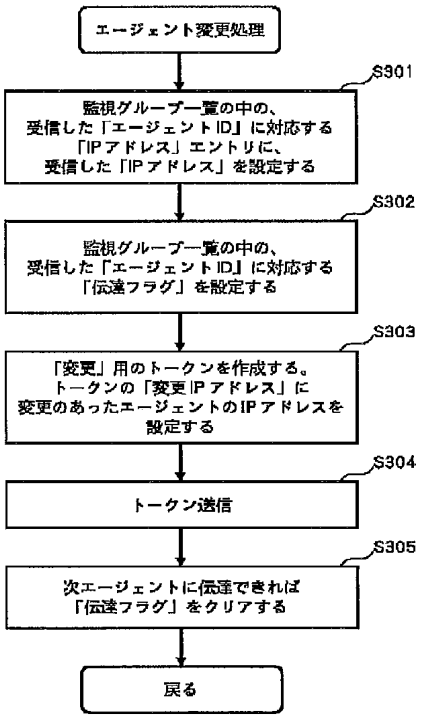
【図４】



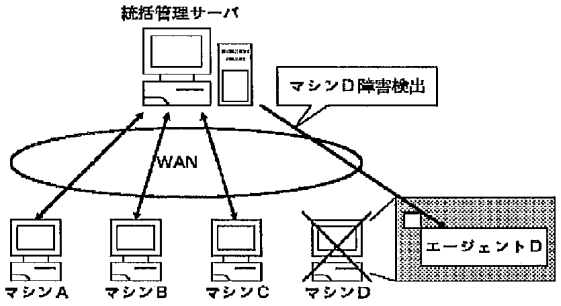
【図５】



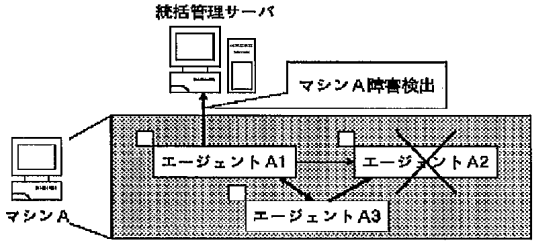
【図７】



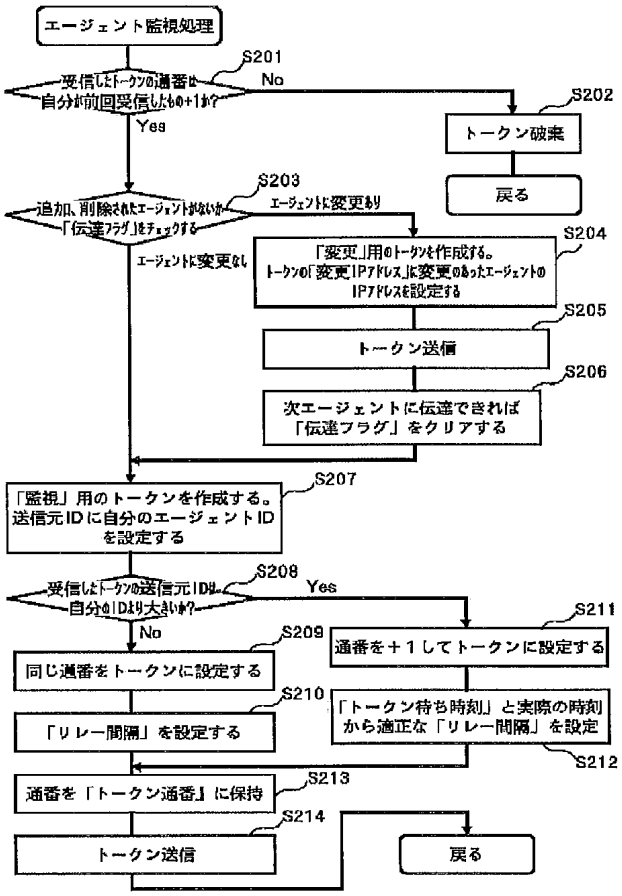
【図９】



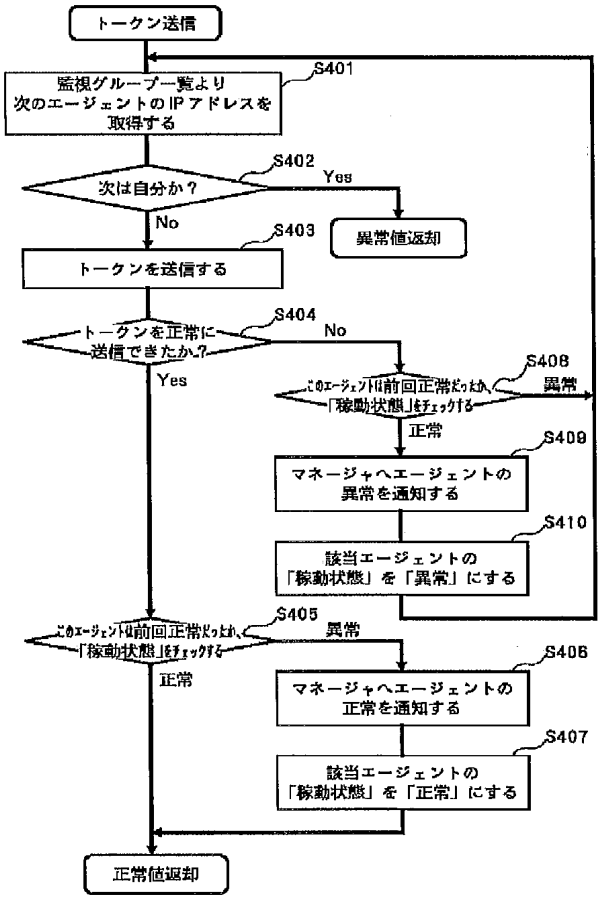
【図１０】



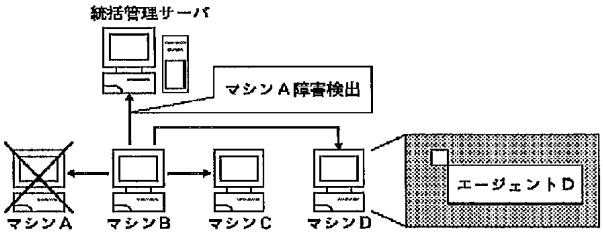
【図６】


エージェント監視処理
S201
受信したトークンの通番は自分が前回受信したもの+1か?
No
Yes
S202
トークン破棄
戻る
S203
追加、削除されたエージェントがないか「伝達フラグ」をチェックする
エージェントに変更あり
エージェントに変更なし
S204
「変更」用のトークンを作成する。トークンの「変更IPアドレス」に変更のあったエージェントのIPアドレスを設定する
S205
トークン送信
S206
次エージェントに伝達できれば「伝達フラグ」をクリアする
S207
「監視」用のトークンを作成する。送信元IDに自分のエージェントIDを設定する
S208
受信したトークンの送信元IDは自分のIDより大きいか?
Yes
No
S209
同じ通番をトークンに設定する
S210
「リレー間隔」を設定する
S211
通番を＋１してトークンに設定する
「トークン待ち時刻」と実際の時刻から適正な「リレー間隔」を設定
S212
S213
通番を「トークン通番」に保持
S214
トークン送信
戻る

【図８】


トークン送信
S401
監視グループ一覧より次のエージェントのIPアドレスを取得する
S402
次は自分か?
Yes
No
異常値返却
S403
トークンを送信する
S404
トークンを正常に送信できたか?
No
Yes
S408
このエージェントは前回正常だったか「稼動状態」をチェックする
異常
正常
S409
マネージャへエージェントの異常を通知する
S410
該当エージェントの「稼動状態」を「異常」にする
S405
このエージェントは前回正常だったか「稼動状態」をチェックする
異常
正常
S406
マネージャへエージェントの正常を通知する
S407
該当エージェントの「稼動状態」を「正常」にする
正常値返却

【図１１】


統括管理サーバ
マシンA障害検出
マシンA
マシンB
マシンC
マシンD
エージェントD